

SonicWALL Internet Security Appliances

# SonicOS 4.0 Enhanced Administrator's Guide

**For the SonicWALL TZ 180 and TZ 190**







# Table of Contents

---

<b>Table of Contents</b> .....	<b>iii</b>
<b>Part 1: Introduction</b>	
<b>Chapter 1: Preface</b> .....	<b>23</b>
Preface .....	23
Copyright Notice .....	23
Trademarks .....	23
Limited Warranty .....	24
About this Guide .....	24
Organization of this Guide .....	25
Guide Conventions .....	27
SonicWALL Technical Support .....	28
More Information on SonicWALL Products .....	28
Current Documentation .....	29
<b>Chapter 2: Common Criteria Guide</b> .....	<b>31</b>
Common Criteria .....	31
Overview of Common Criteria Operation .....	31
Use of GUI Interface for Local Management .....	32
Related Documents .....	33
<b>Chapter 3: Introduction</b> .....	<b>35</b>
Introduction .....	35
What's New in SonicOS Enhanced 4.0 .....	35
SonicWALL Management Interface .....	40

---

## Part 2: System

<b>Chapter 4: Viewing the SonicWALL Security Dashboard</b>	<b>47</b>
System > Security Dashboard	47
SonicWALL Security Dashboard Overview	47
Using the SonicWALL Security Dashboard	50
Related Features	59
<b>Chapter 5: Viewing Status Information</b>	<b>61</b>
System > Status	61
Wizards	61
System Messages	62
System Information	62
Latest Alerts	63
Security Services	63
Registering Your SonicWALL Security Appliance	64
Network Interfaces	66
<b>Chapter 6: Managing SonicWALL Licenses</b>	<b>67</b>
System > Licenses	67
Node License Status	67
Security Services Summary	68
Manage Security Services Online	69
Manual Upgrade	70
Manual Upgrade for Closed Environments	70
<b>Chapter 7: Configuring Administration Settings</b>	<b>73</b>
System > Administration	73
Firewall Name	73
Administrator Name & Password	73
Login Security Settings	74
Multiple Administrators	76
Web Management Settings	77
SSH Management Settings	78
Advanced Management	78
Download URL	82
Selecting UI Language	83

<b>Chapter 8: Managing Certificates</b>	<b>85</b>
System > Certificates	85
Digital Certificates Overview	85
Certificates and Certificate Requests	86
Certificate Details	87
Importing Certificates	87
Deleting a Certificate	89
Certificate Revocation List (CRL)	89
Generating a Certificate Signing Request	90
<b>Chapter 9: Configuring Time Settings</b>	<b>93</b>
System > Time	93
System Time	93
NTP Settings	94
<b>Chapter 10: Setting Schedules</b>	<b>95</b>
System > Schedules	95
Adding a Schedule	97
Deleting Schedules	97
<b>Chapter 11: Managing SonicWALL Security Appliance Firmware</b>	<b>99</b>
System > Settings	99
Settings	100
Firmware Management	100
SafeMode - Rebooting the SonicWALL Security Appliance	103
FIPS	104
<b>Chapter 12: Using SonicWALL Packet Capture</b>	<b>105</b>
System > Packet Capture	105
Packet Capture Overview	105
Using Packet Capture	107
Configuring Packet Capture	111
Verifying Packet Capture Activity	120
Related Information	122

---

**Chapter 13: Using Diagnostic Tools & Restarting the Appliance . . . . 125**

System > Diagnostics . . . . .	125
Tech Support Report . . . . .	126
Diagnostic Tools . . . . .	126
Active Connections Monitor . . . . .	127
CPU Monitor . . . . .	128
DNS Name Lookup . . . . .	129
Find Network Path . . . . .	129
Packet Capture . . . . .	130
Ping . . . . .	131
Process Monitor . . . . .	132
Real-Time Black List Lookup . . . . .	132
Reverse Name Resolution . . . . .	132
Trace Route . . . . .	133
Web Server Monitor . . . . .	133
System > Restart . . . . .	134

**Part 3: Network****Chapter 14: Configuring Interfaces . . . . . 137**

Network > Interfaces . . . . .	137
Setup Wizard . . . . .	138
Interface Settings . . . . .	138
Interface Traffic Statistics . . . . .	139
Interfaces . . . . .	139
SonicOS Enhanced Secure Objects . . . . .	140
Transparent Mode . . . . .	141

Configuring Interfaces .....	141
Configuring the LAN and OPT Interfaces (Static) .....	141
Configuring Advanced Settings for the Interface .....	142
Configuring Interfaces in Transparent Mode .....	143
Configuring Wireless Interfaces .....	145
Configuring a WAN Interface .....	147
Configuring SonicWALL PortShield Interfaces .....	150
Configuring the Wireless WAN Interface .....	152
Managing WWAN Connections .....	153
Specifying the WAN Connection Model .....	153
Configuring Basic Wireless WAN Settings .....	154
Configuring Remotely Triggered Dial-Out on the WWAN .....	156
Configuring the Maximum Allowed WWAN Connections .....	157
Creating a WLAN Subnet .....	157
<b>Chapter 15: Configuring PortShield Interfaces .....</b>	<b>159</b>
SonicWALL PortShield Interfaces .....	159
Security Services with PortShield .....	159
Network > SwitchPorts .....	160
Overview .....	160
Using Different Approaches to Configuration .....	161
Creating a PortShield Interface from the Interfaces Area .....	162
Creating a New Zone for the PortShield Interface .....	166
Refining the PortShield Interface .....	167
Creating Transparent Mode PortShield Interfaces .....	169
Mapping Ports from the Switch Ports Window .....	172
PortShield Deployment Scenario .....	174
Deployment Details .....	175
Configuring the Hospitality Example Deployment .....	176
<b>Chapter 16: Setting Up WAN Failover and Load Balancing .....</b>	<b>181</b>
Network > WAN Failover & Load Balancing .....	181
WAN Failover Caveats .....	181
Setting Up WAN Failover and Load Balancing .....	182
WAN Probe Monitoring .....	186
WAN Load Balancing Statistics .....	189

<b>Chapter 17: Configuring Zones</b> .....	<b>191</b>
Network > Zones .....	191
How Zones Work .....	192
Predefined Zones .....	193
Security Types .....	193
Allow Interface Trust .....	194
Enabling SonicWALL Security Services on Zones .....	194
The Zone Settings Table .....	195
Adding a New Zone .....	196
Deleting a Zone .....	197
Configuring the WLAN Zone .....	197
<b>Chapter 18: Configuring DNS Settings</b> .....	<b>201</b>
Network > DNS .....	201
<b>Chapter 19: Configuring Address Objects</b> .....	<b>203</b>
Network > Address Objects .....	203
Types of Address Objects .....	203
Address Object Groups .....	204
Creating and Managing Address Objects .....	204
Default Address Objects and Groups .....	206
Adding an Address Object .....	209
Editing or Deleting an Address Object .....	210
Creating Group Address Objects .....	211
Public Server Wizard .....	212
Working with Dynamic Addresses .....	212
<b>Chapter 20: Configuring Routes</b> .....	<b>225</b>
Network > Routing .....	225
Route Advertisement .....	226
Route Policies .....	227
Advanced Routing Services (OSPF and RIP) .....	230
Configuring Advanced Routing Services .....	237



<b>Chapter 21: Configuring NAT Policies</b>	<b>245</b>
Network > NAT Policies	245
NAT Policies Table	246
NAT Policy Settings Explained	248
NAT Policies Q&A	249
NAT Load Balancing Overview	250
Creating NAT Policies	254
Using NAT Load Balancing	263
<b>Chapter 22: Managing ARP Traffic</b>	<b>271</b>
Network > ARP	271
Static ARP Entries	272
Secondary Subnets with Static ARP	273
Navigating and Sorting the ARP Cache Table	275
Navigating and Sorting the ARP Cache Table Entries	276
Flushing the ARP Cache	276
<b>Chapter 23: Setting Up the DHCP Server</b>	<b>277</b>
Network > DHCP Server	277
DHCP Server Options Overview	278
DHCP Server Persistence Overview	279
Enabling the DHCP Server	280
DHCP Server Lease Scopes	280
Configuring DHCP Server for Dynamic Ranges	281
Configuring Static DHCP Entries	283
Configuring SonicWALL DHCP Server Options	285
Current DHCP Leases	294
DHCP Option Numbers	294
<b>Chapter 24: Using IP Helper</b>	<b>303</b>
Network > IP Helper	303
IP Helper Settings	303
IP Helper Policies	304
Adding an IP Helper Policy	304
Editing an IP Helper Policy	304
Deleting IP Helper Policies	304

<b>Chapter 25: Setting Up Web Proxy Forwarding</b>	<b>305</b>
Network > Web Proxy	305
Configuring Automatic Proxy Forwarding (Web Only)	305
Bypass Proxy Servers Upon Proxy Failure	306
<b>Chapter 26: Configuring Dynamic DNS</b>	<b>307</b>
Network > Dynamic DNS	307
Supported DDNS Providers	307
Configuring Dynamic DNS	308
Dynamic DNS Settings Table	311
<b>Part 4: Wireless</b>	
<b>Chapter 27: Viewing WLAN Settings, Statistics, and Station Status</b>	<b>315</b>
Wireless Overview	315
Considerations for Using Wireless Connections	316
Recommendations for Optimal Wireless Performance	316
Adjusting the Antennas	317
Wireless Node Count Enforcement	317
MAC Filter List	317
WiFiSec Enforcement	317
Wireless > Status	318
WLAN Settings	319
WLAN Statistics	320
WLAN Activities	320
Station Status	321
<b>Chapter 28: Configuring Wireless Settings</b>	<b>323</b>
Wireless > Settings	323
Wireless Radio Mode	323
Wireless Settings	324
Secure Wireless Bridging	324
Configuring a Secure Wireless Bridge	326
<b>Chapter 29: Configuring WEP and WPA Security</b>	<b>333</b>
Wireless > WEP/WPA Security	333
Authentication Overview	334
WEP Encryption Settings	334
WEP Encryption Keys	335
WPA Encryption Settings	335
WPA/WPA2 Encryption Settings	337

<b>Chapter 30: Configuring Advanced Wireless Settings</b> .....	<b>339</b>
Wireless > Advanced .....	339
Beaconing & SSID Controls .....	340
Wireless Client Communications .....	340
Configurable Antenna Diversity .....	340
Advanced Radio Settings .....	342
<b>Chapter 31: Configuring MAC Filter List</b> .....	<b>345</b>
Wireless > MAC Filter List .....	345
Allow or Deny Specific Resources .....	345
<b>Chapter 32: Configuring Wireless IDS</b> .....	<b>347</b>
Wireless > IDS .....	347
Wireless Bridge IDS .....	347
Access Point IDS .....	348
Enable Client Null Probing .....	348
Association Flood Detection .....	348
Intrusion Detection Settings .....	349
Discovered Access Points .....	349
Scanning for Access Points .....	350
Authorizing Access Points on Your Network .....	350
<b>Chapter 33: Configuring Virtual Access Points</b> .....	<b>351</b>
Wireless > Virtual Access Point .....	351
SonicPoint VAP Overview .....	352
Virtual AP Configuration Task List .....	353
Thinking Critically About VAPs .....	365
Determining Your VAP Needs .....	365
A Sample Network .....	365
Determining Security Configurations .....	366
VAP Configuration Worksheet .....	366

---

## Part 5: WWAN

<b>Chapter 34: Configuring Wireless WAN (TZ 190 only)</b> .....	<b>371</b>
WWAN .....	371
Wireless WAN Overview .....	371
Wireless WAN Prerequisites .....	376
Viewing the WWAN Status .....	377
Configuring Wireless WAN .....	377
Monitoring WWAN Data Usage .....	385
WWAN Glossary .....	386

## Part 6: SonicPoint

<b>Chapter 35: Managing SonicPoints</b> .....	<b>391</b>
SonicPoint > SonicPoints .....	391
Before Managing SonicPoints .....	391
SonicPoint Provisioning Profiles .....	392
<b>Chapter 36: Viewing Station Status</b> .....	<b>401</b>
SonicPoint > Station Status .....	401
<b>Chapter 37: Using and Configuring IDS</b> .....	<b>405</b>
SonicPoint > IDS .....	405
Wireless Intrusion Detection Services .....	405
<b>Chapter 38: Configuring RF Monitoring</b> .....	<b>409</b>
SonicPoint > RF Monitoring .....	409
RF Monitoring Overview .....	409
Enabling RF Monitoring on SonicPoint(s) .....	411
Using The RF Monitoring Interface .....	411
Types of RF Threat Detection .....	414
Practical RF Monitoring Field Applications .....	415

## Part 7: Firewall

<b>Chapter 39: Configuring Access Rules</b> .....	<b>421</b>
Firewall > Access Rules .....	421
Stateful Packet Inspection Default Access Rules Overview .....	422
Using Bandwidth Management with Access Rules Overview .....	422
Configuration Task List .....	423

<b>Chapter 40: Configuring Advanced Access Rule Settings</b> .....	<b>433</b>
Firewall > Advanced .....	433
Detection Prevention .....	434
Dynamic Ports .....	434
Source Routed Packets .....	434
Connections .....	434
Access Rule Service Options .....	435
IP and UDP Checksum Enforcement .....	435
UDP .....	435
<b>Chapter 41: Configuring TCP Settings</b> .....	<b>437</b>
Firewall > TCP Settings .....	437
TCP Traffic Statistics .....	437
TCP Settings .....	438
Working with SYN/RST/FIN Flood Protection .....	439
<b>Chapter 42: Configuring Firewall Services</b> .....	<b>447</b>
Firewall > Services .....	447
Default Services Overview .....	448
Custom Services Configuration Task List .....	448
<b>Chapter 43: Configuring Multicast Settings</b> .....	<b>457</b>
Firewall > Multicast .....	457
Multicast Snooping .....	458
Multicast Policies .....	458
IGMP State Table .....	459
Enabling Multicast on LAN-Dedicated Interfaces .....	460
Enabling Multicast Through a VPN .....	461
<b>Chapter 44: Monitoring Active Connections</b> .....	<b>463</b>
Firewall > Connections Monitor .....	463
Viewing Connections .....	464
Filtering Connections Viewed .....	464

<b>Chapter 45: Managing Quality of Service</b> .....	<b>467</b>
Firewall > QoS Mapping .....	467
Classification .....	467
Marking .....	468
Conditioning .....	468
802.1p and DSCP QoS .....	469
Bandwidth Management .....	479
Outbound Bandwidth Management .....	482
Inbound Bandwidth Management .....	486
Glossary .....	489
<b>Chapter 46: Configuring SSL Control</b> .....	<b>493</b>
Firewall > SSL Control .....	493
Overview of SSL Control .....	493
SSL Control Configuration .....	501
Enabling SSL Control on Zones .....	503
SSL Control Events .....	504
<b>Part 8: VoIP</b>	
<b>Chapter 47: Configuring VoIP Support</b> .....	<b>509</b>
VoIP .....	509
VoIP Overview .....	509
SonicWALL's VoIP Capabilities .....	512
Configuring SonicWALL VoIP Features .....	520
VoIP Deployment Scenarios .....	531
<b>Part 9: VPN</b>	
<b>Chapter 48: Configuring VPN Policies</b> .....	<b>537</b>
VPN > Settings .....	537
VPN Overview .....	537
Configuring VPNs in SonicOS Enhanced .....	542
Configuring GroupVPN Policies .....	552
Site-to-Site VPN Configurations .....	561
Creating Site-to-Site VPN Policies .....	562
VPN Auto-Added Access Rule Control .....	578
<b>Chapter 49: Configuring Advanced VPN Settings</b> .....	<b>581</b>
VPN > Advanced .....	581
Advanced VPN Settings .....	581

<b>Chapter 50: Configuring DHCP Over VPN</b>	<b>587</b>
VPN > DHCP over VPN	587
DHCP Relay Mode	587
Configuring the Central Gateway for DHCP Over VPN	588
Configuring DHCP over VPN Remote Gateway	588
Current DHCP over VPN Leases	591
<b>Chapter 51: Configuring L2TP Server</b>	<b>593</b>
VPN > L2TP Server	593
Configuring the L2TP Server	594
<b>Part 10: User Management</b>	
<b>Chapter 52: Managing Users and Authentication Settings</b>	<b>599</b>
User Management	599
Introduction to User Management	599
Viewing Status on Users > Status	613
Configuring Settings on Users > Settings	614
Configuring Local Users	618
Configuring Local Groups	621
Configuring RADIUS Authentication	625
Configuring LDAP Integration in SonicOS Enhanced	631
Configuring Single Sign-On	641
Configuring Multiple Administrator Support	670
<b>Chapter 53: Managing Guest Services and Guest Accounts</b>	<b>677</b>
Users > Guest Services	677
Global Guest Settings	678
Guest Profiles	678
Users > Guest Accounts	679
Viewing Guest Account Statistics	680
Adding Guest Accounts	680
Enabling Guest Accounts	682
Enabling Auto-prune for Guest Accounts	682
Printing Account Details.	683
Users > Guest Status	683
Logging Accounts off the Appliance	684

---

## Part 11: Security Services

<b>Chapter 54: Managing SonicWALL Security Services</b> .....	<b>687</b>
SonicWALL Security Services .....	687
Security Services Summary .....	688
Managing Security Services Online .....	690
Security Services Settings .....	690
Security Services Information .....	691
Update Signature Manually .....	691
Activating Security Services .....	693
<b>Chapter 55: Configuring SonicWALL Content Filtering Service</b> .....	<b>695</b>
Security Services > Content Filter .....	695
SonicWALL Content Filtering Service .....	696
Content Filter Status .....	696
Content Filter Type .....	697
Restrict Web Features .....	698
Trusted Domains .....	699
CFS Exclusion List .....	699
Message to Display when Blocking .....	700
Configuring SonicWALL Filter Properties .....	700
Custom List .....	700
Consent .....	701
Configuring N2H2 Internet Filtering .....	703
N2H2 Properties .....	703
Configuring SonicWALL Blocking Features .....	704
Configuring Websense Enterprise Content Filtering .....	705
Websense Properties .....	705
Configuring SonicWALL Blocking Features .....	706
<b>Chapter 56: Activating SonicWALL Client Anti-Virus</b> .....	<b>709</b>
Security Services > Anti-Virus .....	709
Activating SonicWALL Client Anti-Virus .....	710
Activating a SonicWALL Client Anti-Virus FREE TRIAL .....	712
Configuring Client Anti-Virus Service .....	712
Security Services > E-mail Filter .....	714



---

## **Chapter 57: Managing SonicWALL Gateway Anti-Virus Service . . . . .715**

Security Services > Gateway Anti-Virus . . . . .	715
SonicWALL GAV Multi-Layered Approach . . . . .	716
HTTP File Downloads . . . . .	718
SonicWALL GAV Architecture . . . . .	718
Creating a mySonicWALL.com Account . . . . .	719
Registering Your SonicWALL Security Appliance . . . . .	721
Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License .	721
Activating FREE TRIALS . . . . .	723
Setting Up SonicWALL Gateway Anti-Virus Protection . . . . .	723
Enabling SonicWALL GAV . . . . .	724
Applying SonicWALL GAV Protection on Interfaces . . . . .	724
Applying SonicWALL GAV Protection on Zones . . . . .	725
Viewing SonicWALL GAV Status Information . . . . .	726
Updating SonicWALL GAV Signatures . . . . .	727
Specifying Protocol Filtering . . . . .	727
Enabling Inbound Inspection . . . . .	727
Enabling Outbound SMTP Inspection . . . . .	728
Restricting File Transfers . . . . .	728
Configuring Gateway AV Settings . . . . .	729
Configuring HTTP Clientless Notification . . . . .	730
Configuring a SonicWALL GAV Exclusion List . . . . .	731
Viewing SonicWALL GAV Signatures . . . . .	732

## **Chapter 58: Activating Intrusion Prevention Service . . . . .735**

Security Services > Intrusion Prevention Service . . . . .	735
SonicWALL Deep Packet Inspection . . . . .	735
How SonicWALL's Deep Packet Inspection Works . . . . .	736
SonicWALL IPS Terminology . . . . .	736
SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation	737
Creating a mySonicWALL.com Account . . . . .	738
Registering Your SonicWALL Security Appliance . . . . .	739
Activating FREE TRIALS . . . . .	740
Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License	740
Setting Up SonicWALL Intrusion Prevention Service Protection . . .	742

<b>Chapter 59: Activating Anti-Spyware Service</b> .....	<b>745</b>
Security Services > Anti-Spyware Service .....	745
SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation	746
Creating a mySonicWALL.com Account .....	747
Registering Your SonicWALL Security Appliance .....	748
Activating FREE TRIALS .....	748
Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License	749
Setting Up SonicWALL Anti-Spyware Service Protection .....	750
<b>Chapter 60: Configuring SonicWALL Real-Time Blacklist</b> .....	<b>753</b>
SMTP Real-Time Black List Filtering .....	753
Security Services > RBL Filter .....	754
Adding RBL Services .....	754
User-Defined SMTP Server Lists .....	755
<b>Chapter 61: Configuring SonicWALL Global Security Client</b> .....	<b>757</b>
Security Services > Global Security Client .....	757
Global Security Client Features .....	758
How SonicWALL Global Security Client Works .....	759
Global Security Client Licensing .....	760
Activating Global Security Client Licenses on Your SonicWALL ..	760
Configuring Security Policies for Global Security Clients .....	761
<b>Part 12: Log</b>	
<b>Chapter 62: Managing Log Events</b> .....	<b>765</b>
Log > View .....	765
Log View Table .....	766
Refresh .....	766
Clear Log .....	767
Export Log .....	767
E-mail Log .....	767
Filtering Log Records Viewed .....	767
Log Event Messages .....	768
<b>Chapter 63: Configuring Log Categories</b> .....	<b>769</b>
Log > Categories .....	769
Log Priority .....	770
Log Categories .....	771

<b>Chapter 64: Configuring Syslog Settings</b> .....	<b>775</b>
Log > Syslog .....	775
Syslog Settings .....	776
Syslog Servers .....	777
<b>Chapter 65: Configuring Log Automation</b> .....	<b>779</b>
Log > Automation .....	779
E-mail Log Automation .....	780
Mail Server Settings .....	780
<b>Chapter 66: Configuring Name Resolution</b> .....	<b>781</b>
Log > Name Resolution .....	781
Selecting Name Resolution Settings .....	781
Specifying the DNS Server .....	782
<b>Chapter 67: Generating Log Reports</b> .....	<b>783</b>
Log > Reports .....	783
Data Collection .....	784
View Data .....	784
<b>Chapter 68: Activating SonicWALL ViewPoint</b> .....	<b>787</b>
Log > ViewPoint .....	787
Activating ViewPoint .....	788
Enabling ViewPoint Settings .....	789
<b>Part 13: Wizards</b>	
<b>Chapter 69: Configuring Internet Connectivity Using the Setup Wizard</b>	<b>793</b>
Wizards > Setup Wizard .....	793
Using the Setup Wizard .....	793
Configuring a Static IP Address with NAT Enabled .....	795
Configuring DHCP Networking Mode .....	800
Configuring NAT Enabled with PPPoE .....	805
Configuring PPTP Network Mode .....	810
<b>Chapter 70: Using the Registration &amp; License Wizard</b> .....	<b>815</b>
Wizards > Registration & License Wizard .....	815
<b>Chapter 71: Configuring a Public Server with the Wizard</b> .....	<b>821</b>
Wizards > Public Server Wizard .....	821

---

<b>Chapter 72: Configuring VPN Policies with the VPN Policy Wizard . .</b>	<b>827</b>
Wizards > VPN Wizard . . . . .	827
Using the VPN Policy Wizard . . . . .	828
Connecting the Global VPN Clients . . . . .	831
Configuring a Site-to-Site VPN using the VPN Wizard . . . . .	832
<b>Index</b> .....	<b>837</b>

# **PART 1**

# **Introduction**





# CHAPTER 1

## Preface

---

## Preface

### Copyright Notice

© 2007 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

### Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

eDirectory and NetWare are registered trademarks of Novell, Inc.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

## Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

**DISCLAIMER OF WARRANTY.** EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

**DISCLAIMER OF LIABILITY.** SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

## About this Guide

Welcome to the *SonicWALL SonicOS Enhanced 4.0 Administrator's Guide*. This manual provides the information you need to successfully activate, configure, and administer SonicOS Enhanced 4.0 for the SonicWALL PRO 4060, PRO 4100, and PRO 5060 security appliances.



**Note**

Always check <<http://www.sonicwall.com/services/documentation.html>> for the latest version of this manual as well as other SonicWALL products and services documentation.

## Organization of this Guide

The *SonicWALL SonicOS Enhanced 4.0 Administrator's Guide* organization is structured into the following parts that follow the SonicWALL Web Management Interface structure. Within these parts, individual chapters correspond to SonicWALL security appliance management interface layout.

### Part 1 Introduction

This part provides an overview of new SonicWALL SonicOS Enhanced features, guide conventions, support information, and an overview of the SonicWALL security appliance management interface.

### Part 2 System

This part covers a variety of SonicWALL security appliance controls for managing system status information, registering the SonicWALL security appliance, activating and managing SonicWALL Security Services licenses, configuring SonicWALL security appliance local and remote management options, managing firmware versions and preferences, and using included diagnostics tools for troubleshooting.

### Part 3 Network

This part covers configuring the SonicWALL security appliance for your network environment. The **Network** section of the SonicWALL Management Interface includes:

- **Interfaces** - configure logical interfaces for connectivity.
- **WAN Failover and Load Balancing** - configure one of the user-defined interfaces to act as a secondary WAN port for backup or load balancing.
- **Zones** - configure security zones on your network.
- **DNS** - set up DNS servers for name resolution.
- **Address Objects** - configure host, network, and address range objects.
- **Routing** - view the **Route Table**, **ARP Cache** and configure static and dynamic routing by interface.
- **NAT Policies** - create NAT policies including One-to-One NAT, Many-to-One NAT, Many-to-Many NAT, or One-to-Many NAT.
- **ARP** - view the ARP settings and clear the ARP cache as well as configure ARP cache time.
- **DHCP Server** - configure the SonicWALL as a DHCP Server on your network to dynamically assign IP addresses to computers on your LAN or DMZ zones.
- **IP Helper** - configure the SonicWALL to forward DHCP requests originating from the interfaces on the SonicWALL to a centralized server on behalf of the requesting client.
- **Web Proxy** - configure the SonicWALL to automatically forward all Web proxy requests to a network proxy server.

- **Dynamic DNS** - configure the SonicWALL to dynamically register its WAN IP address with a DDNS service provider.

## Part 4 SonicPoint

The part covers the configuration of the SonicWALL security appliance for provisioning and managing SonicWALL SonicPoints as part of a SonicWALL Distributed Wireless Solution.

## Part 5 Firewall

This part covers tools for managing how the SonicWALL security appliance handles traffic through the firewall.

## Part 6 VoIP

This part provides instructions for configuring the SonicWALL security appliance to support H.323 or SIP Voice over IP (VoIP) connections.

## Part 7 Application Firewall

Application firewall is a set of application-specific policies that gives you granular control over network traffic on the level of users, email users, schedules, and IP-subnets. The primary functionality of this application-layer access control feature is to regulate Web browsing, file transfer, email, and email attachments.

## Part 8 VPN

This part covers how to create VPN policies on the SonicWALL security appliance to support SonicWALL Global VPN Clients as well as creating site-to-site VPN policies for connecting offices running SonicWALL security appliances.

## Part 9 Users

This part covers how to configure the SonicWALL security appliance for user level authentication as well as manage guest services for managed SonicPoints.

## Part 10 Hardware Failover

This part explains how to configure the SonicWALL security appliance for failover to another SonicWALL security appliance in the event of hardware failure.

## Part 11 Security Services

This part includes an overview of available SonicWALL Security Services as well as instructions for activating the service, including FREE trials. These subscription-based services include SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, SonicWALL Content Filtering Service, SonicWALL Client Anti-Virus, and well as other services.

## Part 12 Log

This part covers managing the SonicWALL security appliance's enhanced logging, alerting, and reporting features. The SonicWALL security appliance's logging features provide a comprehensive set of log categories for monitoring security and network activities.

## Part 13 Wizards

This part walks you through using the SonicWALL Configuration Wizards for configuring the SonicWALL security appliance for LAN to WAN (Internet) connectivity, settings up public servers for Internet connectivity behind the firewall, and setting GroupVPN and site-to-site VPN policies for establishing VPN connections for remote SonicWALL Global VPN Client users or remote offices with a SonicWALL security appliance for LAN to LAN connections.

The SonicWALL Configuration Wizards in SonicOS Enhanced 4.0 include:

- The **Setup Wizard** takes you step by step through network configuration for Internet connectivity. There are four types of network connectivity available: Static IP, DHCP, PPPoE, and PPTP.
- The **Registration & License Wizard** simplifies the process of registering your SonicWALL security appliance and obtaining licenses for additional security services.
- The **Public Server Wizard** takes you step by step through adding a server to your network, such as a mail server or a web server. The wizard automates much of the configuration you need to establish security and access for the server.
- The **VPN Policy Wizard** steps you through the configuration of Group VPNs and site-to-site VPNs.

## Guide Conventions

The following conventions used in this guide are as follows:

Convention	Use
Bold	Highlights items you can select on the SonicWALL security appliance management interface.
Italic	Highlights a value to enter into a field. For example, "type <i>192.168.168.168</i> in the <b>IP Address</b> field."
Menu Item > Menu Item	Indicates a multiple step Management Interface menu choice. For example, <b>Security Services &gt; Content Filter</b> means select <b>Security Services</b> , then select <b>Content Filter</b> .

## Icons Used in this Manual

These special messages refer to noteworthy information, and include a symbol for quick identification:

---

**Caution** Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL.

---



Tip

---

Useful information about security features and configurations on your SonicWALL.

---



Note

---

Important information on a feature that requires callout for special attention.

---

## SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/us/Support.html>. Web-based resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

To contact SonicWALL telephone support, see the telephone numbers listed below:

### North America Telephone Support

**U.S./Canada** - 888.777.1476 or +1 408.752.7819

### International Telephone Support

**Australia** - + 1800.35.1642

**Austria** - + 43(0)820.400.105

**EMEA** - +31(0)411.617.810

**France** - + 33(0)1.4933.7414

**Germany** - + 49(0)1805.0800.22

**Hong Kong** - + 1.800.93.0997

**India** - + 8026556828

**Italy** - +39.02.7541.9803

**Japan** - + 81(0)3.5460.5356

**New Zealand** - + 0800.446489

**Singapore** - + 800.110.1441

**Spain** - + 34(0)9137.53035

**Switzerland** - +41.1.308.3.977

**UK** - +44(0)1344.668.484

## More Information on SonicWALL Products

Contact SonicWALL, Inc. for information about SonicWALL products and services at:

Web:<http://www.sonicwall.com>

E-mail:[sales@sonicwall.com](mailto:sales@sonicwall.com)

Phone:(408) 745-9600

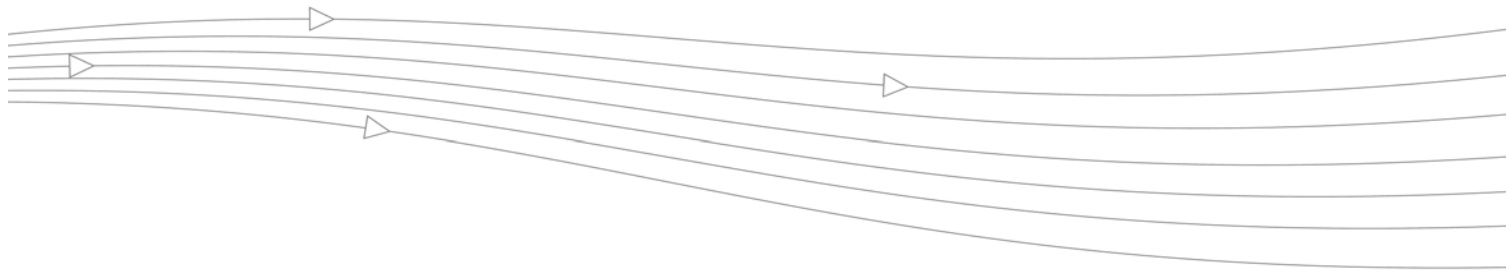
Fax:(408) 745-9300

## Current Documentation

Check the SonicWALL documentation Web site for that latest versions of this manual and all other SonicWALL product documentation.

<http://www.sonicwall.com/us/Support.html>





# CHAPTER 2

## Common Criteria Guide

---

### Common Criteria

The purpose of this chapter is to define the Common Criteria-compliant operation of SonicWALL Internet Security Appliances.

Common Criteria is an information technology (IT) validation scheme adopted by the National Information Assurance Partnership (NIAP). NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). NIAP has established the Common Criteria Evaluation Validated Scheme (CCEVS) to validate IT products. Common Criteria is also referred to as ISO 15408.

### Overview of Common Criteria Operation

The Common Criteria evaluated configuration of SonicWALL Internet Security Appliances uses only the firewall services of the device. The VPN services of the device are not included in the Common Criteria evaluated configuration. The Common Criteria evaluated configuration includes all features except those that are explicitly excluded.

The following features are not included in the Common Criteria evaluated configuration:

- VPN
- IPsec or L2TP
- LDAP or RADIUS user authentication
- Security Services
  - Content Filtering Service
  - Client Anti-Virus
  - E-mail Filter
  - Anti-Spyware
  - RBL Filter
  - Global Security Client
  - Intrusion Prevention System
  - Gateway Anti-Virus

- GMS Remote Management
- Syslog Logging
- SonicPoint
- Hardware Failover

Before installing the SonicWALL Internet Security Appliance, the device should be examined for evidence of tampering. Each device includes a tamper-evident seal to prevent access to the inside of the unit. Verify that the tamper evident seal is intact. If there is a sign of tampering, contact SonicWALL Support Services by phone at 888.777.1476 or 408.752.7819.

The GUI management interface is used to administer the device. The use of the GUI management interface is discussed in the “*Use of GUI Interface for Local Management*” section below.

The Common Criteria evaluated configuration only supports SonicOS Enhanced 4.0. You can verify that the device is running SonicOS Enhanced 4.0 from the **System -> Status** page of the management GUI under the **System Information** table, **Firmware Version** entry.

## Use of GUI Interface for Local Management

This section describes the use of the SonicWALL Graphical User Interface (GUI) interface for local management. Using the red cross-over cable supplied with SonicWALL Internet Security Appliances and a management PC, the SonicWALL GUI can be used for local configuration. This provides a secure way of administering the device without the possibility of traffic between the management PC and device being captured or traced. Following the instructions below will insure that only the management PC, directly connected to the device, can be used for management.

Follow the instructions in the SonicOS Getting Started Guide section 2, Connecting the Network Cables, to connect a management PC to the device.

Follow the instructions in the SonicOS Getting Started Guide section 2, Configuring Your Management Station and Accessing The Management Interface to access the management interface of the device

Select an interface to be used as the local management interface. For example, on a PRO series appliance, select X2 or X3.

Use the Add button on the **Network -> Zones** page to add a “Local Management” with a Security Type of Trusted. On the **Network -> Interfaces** page, configure the local management interface. Set the Zone to “Local Management”. Set the IP Address to 192.168.1.1. Set the Subnet Mask to 255.255.255.0. Enable HTTP Management. Log out from the GUI management interface using the Logout button.

Connect the red cross-over cable to the local interface. Configure the management PC's IP address to be 192.168.1.2 with a netmask of 255.255.255.0. Use the management PC's browser to access the device's management interface at <http://192.168.1.2>.

Use the Configure icon on the **Network -> Interfaces** page to configure the LAN interface. Disable HTTP and HTTPS management.

Do not enable HTTP or HTTPS management on any interface other than the local management interface. HTTP and HTTPS management is disabled on all other interfaces by default.

The management PC can now be used to locally administer the device in a secure manner.



## Related Documents

Several other SonicWALL documents provide information relating to the Common Criteria evaluated configuration of SonicWALL Internet Security Appliances. Those documents are described here.

## SonicOS Log Events Reference Guide

During the operation of a SonicWALL security appliance, SonicOS software sends log event messages to the console. Event logging automatically begins when the SonicWALL security appliance is powered on and configured. SonicOS Enhanced supports a traffic log containing entries with multiple fields.

Log event messages provide operational informational and debugging information to help you diagnose problems with communication lines, internal hardware, or your firmware configuration.

**Note**

---

Not all log event messages indicate operational issues with your SonicWALL security appliance.

---

The **Log > View** console display provides log event messages including the following fields for alert notification:

- **Time**—Displays the hour and minute the event occurred.
- **Priority**—Displays the level urgency for the event.
- **Category**—Displays the event type.
- **Message**—Displays a description of the event.
- **Source**—Displays the source IP address of incoming IP packet.
- **Destination**—Displays the destination IP address of incoming IP packet.
- **Note**—Displays displays additional information specific to a particular event occurrence.
- **Rule**—Displays the source and destination zones for the access rule. This field provides a link to the access rule defined in the **Firewall > Access Rules** page.

The display fields for a log event message provides you with data to verify your configurations, trouble-shoot your security appliance, and track IP traffic.





## CHAPTER 3

# Introduction

---

## Introduction

SonicOS Enhanced 4.0 is the most powerful SonicOS operating system designed for the SonicWALL PRO 4060, and the PRO 5060.

## What's New in SonicOS Enhanced 4.0

SonicOS Enhanced 4.0 introduces these new features:

- **Strong SSL and TLS Encryption** - The internal SonicWALL Web server now only supports SSL version 3.0 and TLS with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128 bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 roll-back vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.



**Tip**

---

By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL recommends using these most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0. In Internet Explorer, go to **Tools > Internet Options**, click on the **Advanced** tab, and scroll to the bottom of the **Settings** menu. In Firefox, go to **Tools > Options**, click on the **Advanced** tab, and then click on the **Encryption** tab.

---

- **Single Sign-On User Authentication** - SonicOS Enhanced 4.0 introduces Single Sign-On User Authentication, which provides privileged access to multiple network resources with a single workstation login. Single Sign-On uses the SonicWALL SSO Agent to identify user activity based on workstation IP addresses. Access to resources is based on policy for the group to which the user belongs.
- **Stateful Hardware Failover** - SonicOS Enhanced 4.0 introduces Stateful Hardware Failover, which provides improved failover performance. With Stateful Hardware Failover, the primary and backup security appliances are continuously synchronized so that the backup can seamlessly assume all network responsibilities if the primary appliance fails, with no interruptions to existing network connections. Once the primary and backup

appliances have been associated as a hardware failover pair on mysonicwall.com, you can enable this feature by selecting Enable Stateful Synchronization in the **Hardware Failover > Advanced** page.

- **Application Firewall** - SonicOS Enhanced 4.0 introduces Application Firewall, which provides a way to create application-specific policies to regulate Web browsing, file transfer, email, and email attachments. Application Firewall enables application layer bandwidth management, and also allows you to create custom policies for any protocol. It gives you granular control over network traffic on the level of users, email users, and IP subnets.
- **HTTPS Filtering** - SonicOS Enhanced 4.0 uses HTTPS Filtering to allow administrators to control user access to Web sites when using the encrypted HTTPS protocol. HTTPS Filtering is based on the ratings of Web sites, such as Gambling, Online Banking, Online Brokerage and Trading, Shopping, and Hacking/Proxy Avoidance.

**Note**

---

HTTPS Filtering is IP-based, so IP addresses must be used rather than domain names in the Allowed or Forbidden lists. You can use the **nslookup** command in a DOS cmd window to convert a domain name to its IP address(es). There may be more than one IP address associated with a domain, and if so, all must be added to the Allowed or Forbidden list.

---

- **SSL Control** - SonicOS Enhanced 4.0 introduces SSL Control, which is a system that provides visibility into the handshake of Secure Socket Layer (SSL) sessions, and a method for configuring policies to control the establishment of SSL sessions.
- **Certificate Blocking** - SonicOS Enhanced 4.0 provides a way to specify which HTTPS certificates to block. This feature is closely integrated with SSL Control.
- **Inbound NAT Load Balancing with Server Monitoring** - SonicOS Enhanced 4.0 introduces Inbound NAT Load Balancing with Server Monitoring, which detects when a server is unavailable and stops forwarding requests to it. Inbound NAT Load Balancing spreads the load across two or more servers. When Stateful High Availability (Stateful Hardware Failover) is configured, during a failover, SonicOS forwards all requests to the alternate server(s) until it detects that the offline server is back online. Inbound NAT Load Balancing also works with SonicWALL SSL-VPN appliances.
- **Security Dashboard Web Page** - SonicOS Enhanced 4.0 includes the Security Dashboard page in the user interface, which displays a summary of threats stopped by the SonicWALL security appliance. The Security Dashboard shows two types of reports:
  - A Global Report that displays a summary of threat data received from all SonicWALL security appliances worldwide.
  - An Individual Appliance Report that displays a summary of attacks detected by the local SonicWALL security appliance.
- **Registration & License Wizard** - As part of the new Security Dashboard, SonicOS Enhanced 4.0 provides a License Wizard for both firewall registration and the purchase of security service licenses. The available security services are the same as those that enable Global Reports by providing threat data from SonicWALL devices around the world.
- **Multiple SSH Support** - SonicOS Enhanced 4.0 provides support for multiple concurrent SSH sessions on the SonicWALL security appliance. When connected over SSH, you can run command line interface (CLI) commands to monitor and manage the device. The number of concurrent SSH sessions is determined by device capacity. Note that only one session at a time can configure the SonicWALL, whether the session is on the GUI or the

CLI (SSH or serial console). For instance, if a CLI session goes to the config level, it will ask you if you want to preempt an administrator who is at config level in the GUI or an SSH session.

- **Multiple and Read-only Administrator Login** - SonicOS Enhanced 4.0 introduces Multiple Administrator Login, which provides a way for multiple users to be given administration rights, either full or read-only, for the SonicOS security appliance. Additionally, SonicOS Enhanced 4.0 allows multiple users to concurrently manage the appliance, but only one user at a time can be in config mode with the ability to change configuration settings. This feature applies to both the graphical user interface (GUI) and the command line interface (CLI).
- **IP-Based Connection Limit** - SonicOS Enhanced 4.0 provides a way to limit the number of connections on a per-source or per-destination IP address basis. This feature protects against worms on the LAN side that initiate large numbers of connections in denial of service attacks.
- **IKEv2 Secondary Gateway Support** - SonicOS Enhanced 4.0 introduces IKEv2 Secondary Gateway Support, which provides a way to configure a secondary VPN gateway to act as an alternative tunnel end-point if the primary gateway becomes unreachable. While using the secondary gateway, SonicOS can periodically check for availability of the primary gateway and revert to it, if configured to do so. Configuration for the secondary VPN gateway is available under **VPN > Settings > Add Policy** in the management interface.
- **IKEv2 Dynamic Client Support** - SonicOS Enhanced 4.0 introduces IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:
  - DH Group: 1, 2, or 5
  - Encryption: DES, 3DES, AES-128, AES-192, AES-256
  - Authentication: MD5, SHA1
- These settings are available by pressing the Configure button in the **VPN > Advanced** screen of the management interface. However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.




---

**Note** The VPN policy on the remote gateway must also be configured with the same settings.

---

- **Wireless IDS Rogue Detection** - SonicOS Enhanced 4.0 supports wireless intrusion detection on SonicPoint devices. Wireless IDS Rogue Detection allows you to configure a set of authorized access points, defined by address object groups. If contact is attempted from an unauthorized access point, SonicOS generates an alert.
- **RF Management** - SonicOS Enhanced 4.0 introduces Radio Frequency Management on SonicPoint devices. RF Management provides detection of eleven types of wireless threats:
  - Long duration attack
  - Management frame flood
  - Null probe request
  - Broadcasting de-authentication
  - Valid station with invalid SSID

- Ad-Hoc station
- Unassociated station
- Wellenreiter attack
- NetStumbler attack
- EAPOL packet flood
- Weak WEP IV
- **SMTP Authentication** - SonicOS Enhanced 4.0 supports RFC 2554, which defines an SMTP service extension that allows the SMTP client to indicate an authentication method to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. This feature helps prevent viruses that attack the SMTP server on port 25.
- **Generic DHCP Option Support** - SonicOS Enhanced 4.0 supports generic DHCP configuration, which allows vendor-specific DHCP options in DHCP server leases.
- **DHCP Server Lease Cross-Reboot Persistence** - SonicOS Enhanced 4.0 introduces DHCP Server Lease Cross-Reboot Persistence, which provides the ability to record and return to DHCP server lease bindings across power cycles. The SonicWALL security appliance does not have to depend on dynamic network responses to regain its IP address after a reboot or power cycle. This feature is supported on all SonicWALL PRO platforms. It is not supported on SonicWALL TZ platforms.
- **Custom IP Type Service Objects** - SonicOS Enhanced 4.0 introduces support for Custom IP Type Service Objects, allowing administrators to augment the pre-defined set of Service Objects.
- **Dynamic Address Objects** - SonicOS Enhanced 4.0 supports two changes to Address Objects:
  - **MAC** - SonicOS Enhanced 4.0 will resolve MAC AOs to an IP address by referring to the ARP cache on the SonicWALL.
  - **FQDN** - Fully Qualified Domain Names (FQDN), such as 'www.sonicwall.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the SonicWALL. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.
- **Virtual Access Points** - A "Virtual Access Point" (VAP) is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when there is actually only a single physical AP. Before Virtual AP feature support, wireless networks were relegated to a one-to-one relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. For example, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients. If Open or WPA-EAP were required, they would need to have been provided by a separate, distinctly configured APs. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

In SonicOS Enhanced 4.0, VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously. You can configure up to eight VAPs per SonicPoint access point.

- **Layer 2 Bridge Mode** - SonicOS Enhanced 4.0 supports Layer 2 (L2) Bridge Mode, a new method of unobtrusively integrating a SonicWALL security appliance into any Ethernet network. L2 Bridge Mode is similar to the SonicOS Enhanced Transparent Mode in that it enables a SonicWALL security appliance to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWALL Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti-Virus, and Gateway Anti Spyware.

The following feature enhancements are included in SonicOS Enhanced 4.0:

- **Enhanced Packet Capture** - SonicOS Enhanced 4.0 provides an enhanced version of the Packet Capture feature. Enhanced Packet Capture contains improvements in both functionality and flexibility, including the following:
  - Capture control mechanism with improved granularity for custom filtering
  - Display filter settings independent from capture filter settings
  - Packet status indicating dropped, forwarded, generated, or consumed
  - Three-window output in the user interface that provides the packet list, decoded output of selected packet, and hexadecimal dump of selected packet
  - Export capabilities that include text, HTML, hex dump, and CAP file format
  - Automatic buffer export to FTP server when full
  - Bidirectional packet capture based on IP address and port
  - Configurable wrap-around of capture buffer when full
- **User Authentication** - There are a number of enhancements to user authentication in SonicOS Enhanced 4.0, including optional case-sensitive user names, optional enforcement of unique login names, support for MSCHAP version 2, and support for VPN and L2TP clients changing expired passwords (when that is supported by the back-end authentication server and protocols used). Note that for this purpose there is a new setting on the **VPN > Advanced** page to cause RADIUS to be used in MSCHAP mode when authenticating VPN client users.
- **IP Helper Scalability** - SonicOS Enhanced 4.0 provides enhancements to the IP Helper architecture to support large networks. Improvements include changes to DHCP relay and Net-BIOS functionality. DHCP relay over VPN is now fully integrated.
- **Diagnostics Page Tool Tips** - SonicOS Enhanced 4.0 incorporates self-documenting mouse-over descriptions for diagnostic controls in the graphical user interface.

- **BWM Rate Limiting** - SonicOS Enhanced 4.0 enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.
- **DHCP Client Reboot Behavior Control** - In SonicOS Enhanced 4.0 you can configure the WAN DHCP client to perform a DHCP RENEW or a DHCP DISCOVERY query when attempting to obtain a lease. The previous behavior was to always perform a RENEW, which caused lease failures on some networks, particularly certain cable modem service providers. The new behavior is to perform a DISCOVERY, but it is configurable.
- A checkbox has been added to the **Network > Interfaces > WAN > DHCP Client** page:
  - **Enabled:** when the appliance reboots, the DHCP client performs a DHCP RENEW query.
  - **Disabled:** (Default) when the appliance reboots, the DHCP client performs a DHCP DISCOVERY query.
- **Dynamic Route Metric Recalculation Based on Interface Availability** - To better support redundant or multiple path Advanced Routing configurations, when a default-route's interface is unavailable (due to no-link or negative WAN LB probe response), that default route's metric will be changed to 255, and the route will be instantly disabled. When a default-route's interface is again determined to be available, its metric will be changed back to 20, and the route will be non-disruptively enabled.

## SonicWALL Management Interface

The SonicWALL security appliance's Web-based management interface provides a easy-to-use graphical interface for configuring your SonicWALL security appliance. The following provides an overview of the key management interface objects.

The screenshot shows the SonicWALL Management Interface. The left sidebar contains navigation options: System, Network, SonicPoint, Firewall, VoIP, VPN, Users, Hardware Failover, Security Services, Log, Wizards, Help, and Logout. The main content area is titled 'System > Status' and includes a 'Wizards...' button. It features several sections: 'System Messages' with warnings about HTTP/HTTPS management and password changes; 'System Information' with details like Model (PRO 5050), Serial Number (000B11247D6), Authentication Code (6CEY-AV8K), Firmware Version (SonicOS Enhanced 3.0.0-20a), ROM Version (SonicROM 2.4.0.0), CPU (10s average: 0.00% - 3.40Hz Intel Xeon Processor), Total Memory (512MB RAM, 64MB Flash), Up Time (0 Days 00:20:51), Current Connections (16), and Last Modified By (Unmodified since reboot); 'Security Services' with 'Nodes/Users: Unlimited Nodes' and a registration prompt; and 'Network Interfaces' with a table showing LAN and WAN interfaces.

Name	IP Address	Link Status
X0 (LAN)	192.168.168.168	No link
X1 (WAN)	10.0.93.56	100 Mbps half-Duplex

At the bottom left, the status is 'Ready'.



## Navigating the Management Interface

Navigating the SonicWALL management interface includes a hierarchy of menu buttons on the navigation bar (left side of your browser window). When you click a menu button, related management functions are displayed as submenu items in the navigation bar.



To navigate to a submenu page, click the link. When you click a menu button, the first submenu item page is displayed. The first submenu page is automatically displayed when you click the menu button. For example, when you click the **Network** button, the **Network > Settings** page is displayed.

## Status Bar

The **Status** bar at the bottom of the management interface window displays the status of actions executed in the SonicWALL management interface.



Status: Ready

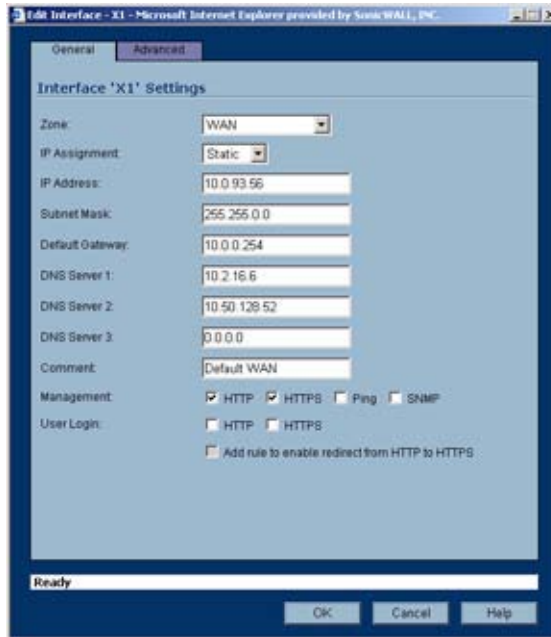
## Applying Changes

Click the **Apply** button at the top right corner of the SonicWALL management interface to save any configuration changes you made on the page.



Apply

If the settings are contained in a secondary window within the management interface, when you click **OK**, the settings are automatically applied to the SonicWALL security appliance.



## Navigating Tables

Navigate tables in the management interface with large number of entries by using the navigation buttons located on the upper right top corner of the table.




#	Time	Message	Source	Destination	Notes	Rule
1	10/14/2004 09:51:44.054	Web management request allowed	10.0.202.62, 1785, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
2	10/14/2004 09:51:06.794	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
3	10/14/2004 09:50:07.352	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
4	10/14/2004 09:49:08.768	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
5	10/14/2004 09:48:09.176	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
6	10/14/2004 09:47:10.484	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
7	10/14/2004 09:46:11.896	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
8	10/14/2004 09:45:12.176	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
9	10/14/2004 09:44:12.672	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
10	10/14/2004 09:43:14.032	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
11	10/14/2004 09:42:14.384	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
12	10/14/2004 09:41:14.736	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
13	10/14/2004 09:40:16.048	UDP packet dropped	10.0.0.252, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
14	10/14/2004 09:39:33.560	Web management request allowed	10.0.202.62, 1734, WAN	192.168.168.168, 443, LAN	TCP HTTPS	
15	10/14/2004 09:39:17.560	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	
16	10/14/2004 09:38:18.912	UDP packet dropped	10.0.0.253, 1985, WAN	224.0.0.2, 1985, WAN	UDP Port: 1985	

The table navigation bar includes buttons for moving through table pages.




## Common Icons in the Management Interface

The following describe the functions of common icons used in the SonicWALL management interface:

- Clicking on the edit  icon displays a window for editing the settings.
- Clicking on the delete  icon deletes a table entry
- Moving the pointer over the comment  icon displays text from a **Comment** field entry.

## Getting Help

Each SonicWALL security appliance includes Web-based on-line help available from the management interface.

Clicking the question mark  button on the top-right corner of every page accesses the context-sensitive help for the page.



### Tip

---

Accessing the SonicWALL security appliance online help requires an active Internet connection.

---

## Logging Out

The **Logout** button at the bottom of the menu bar terminates the management interface session and displays the authentication page for logging into the SonicWALL security appliance.

A rectangular button with a light blue background and a dark border, containing the text "Logout".

Logout



# **PART 2**

# **System**





## CHAPTER 4

# Viewing the SonicWALL Security Dashboard

---

## System > Security Dashboard

This chapter describes how to use the SonicWALL Security Dashboard feature on a SonicWALL security appliance. This chapter contains the following sections:

- [“SonicWALL Security Dashboard Overview” on page 47](#)
  - [“What is the Security Dashboard?” on page 48](#)
  - [“Benefits” on page 49](#)
  - [“How Does the Security Dashboard Work?” on page 50](#)
  - [“Platforms” on page 50](#)
- [“Using the SonicWALL Security Dashboard” on page 50](#)
  - [“Administrator Prerequisites” on page 50](#)
  - [“Administrator Configuration Tasks” on page 50](#)
- [“Related Features” on page 59](#)

## SonicWALL Security Dashboard Overview

This section provides an introduction to the Security Dashboard feature. This section contains the following subsections:

- [“What is the Security Dashboard?” on page 48](#)
- [“Benefits” on page 49](#)
- [“How Does the Security Dashboard Work?” on page 50](#)
- [“Platforms” on page 50](#)

After reading the Security Dashboard Overview section, you will be familiar with this feature and its benefits.

## What is the Security Dashboard?

The SonicWALL Security Dashboard provides reports of the latest threat protection data from a single SonicWALL appliance and aggregated threat protection data from SonicWALL security appliances deployed globally. The SonicWALL Security Dashboard displays automatically upon successful authentication to a SonicWALL security appliance, and can be viewed at any time by navigating to the **System > Security Dashboard** menu in the left-hand menu.

Reports in the Security Dashboard include:

- Viruses Blocked by SonicWALL Network
- Intrusions Prevented by SonicWALL Network
- Spyware Blocked by SonicWALL Network
- Multimedia (IM/P2P) Detected/Blocked by SonicWALL Network

Each report includes a graph of threats blocked over time and a table of the top blocked threats. Reports, which are updated hourly, can be customized to display data for the last 12 hours, 14 days, 21 days, or 6 months. For easier viewing, SonicWALL Security Dashboard reports can be transformed into a PDF file format with the click of a button.

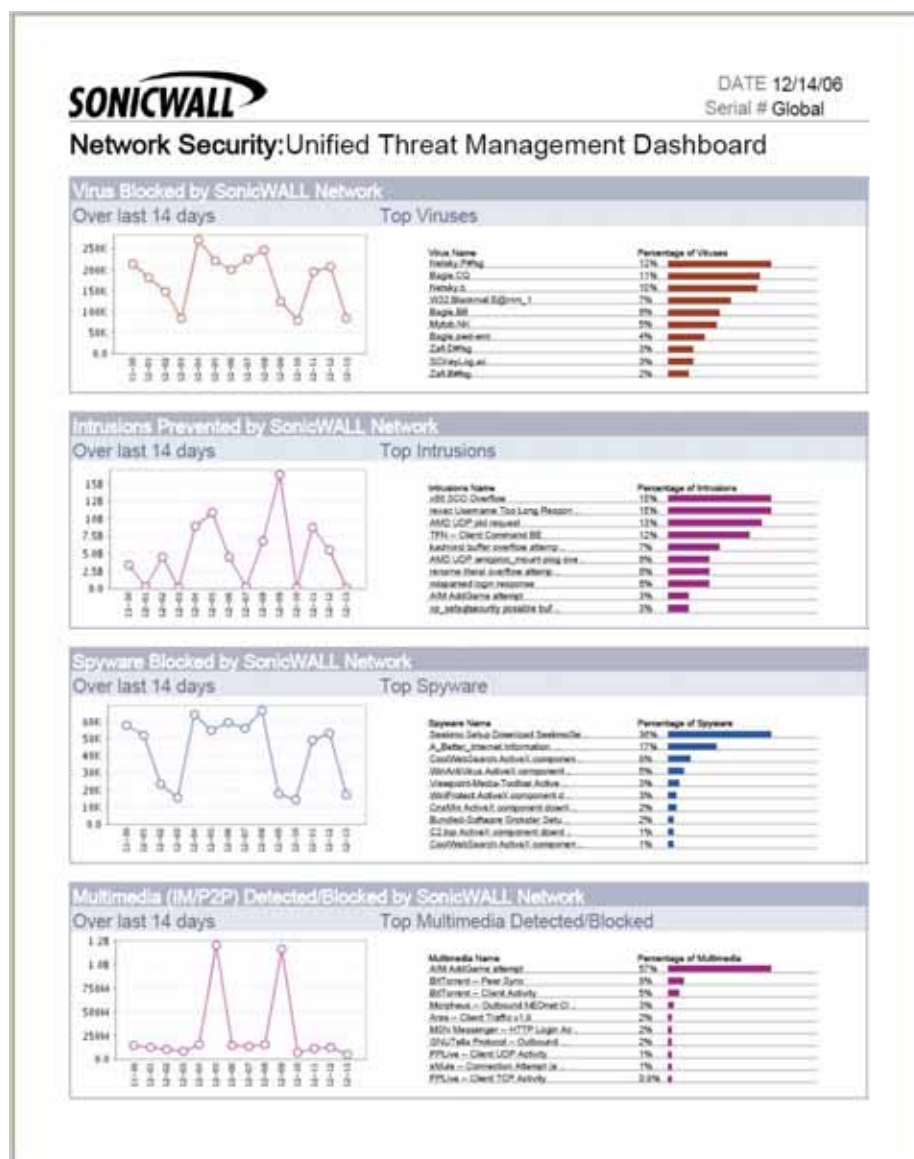




## Benefits

The Security Dashboard provides the latest threat protection information to keep you informed about potential threats being blocked by SonicWALL security appliances. If you subscribe to SonicWALL's security services, including Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention Service (IPS), and Content Filtering Service, you are automatically protected from the threats reported by the SonicWALL Security Dashboard. SonicWALL's security services include ongoing new signature updates to protect against the latest virus and spyware attacks. For information about activating SonicWALL security services, refer to the "Purchasing Security Services" on page 52.

The Security Dashboard provides insight into threats over time, and can be configured to display data from multiple time periods. The SonicWALL Security Dashboard can be viewed easily in the **System > Security Dashboard** page of the SonicWALL appliance management interface, or as a custom generated PDF file.



## How Does the Security Dashboard Work?

The SonicWALL Security Dashboard provides global and appliance-level threat protection statistics. At the appliance level, threat protection data from your SonicWALL security appliance is displayed. At the global level, the SonicWALL Security Dashboard is updated hourly from the SonicWALL backend server with aggregated threat protection data from globally-deployed SonicWALL security appliances. Data provided by the SonicWALL backend server is cached locally for reliable delivery.

**Note**

---

The SonicWALL security appliance must have Internet connectivity (including connection to a DNS server) to receive the latest threat protection statistics from the SonicWALL backend server, which reports aggregated data from globally deployed SonicWALL security appliances. If you lose connectivity, cached data from the last update will display, and the latest data will not be available until connectivity is restored.

---

## Platforms

The Security Dashboard is available on the SonicWALL security appliances running SonicOS 3.5 firmware and higher.

## Using the SonicWALL Security Dashboard

This section contains the following subsections:

- “Administrator Prerequisites” on page 50
- “Administrator Configuration Tasks” on page 50

## Administrator Prerequisites

SonicWALL security appliances running SonicOS 3.5 firmware or later must be set up and registered on [mysonicwall.com](http://mysonicwall.com). For registration instructions, refer to the SonicWALL *Getting Started Guide* for your security appliance, available on the Web at: <http://www.sonicwall.com/us/Support.html>.

**Note**

---

The SonicWALL security appliance must be configured for Internet connectivity and be connected to the Internet to display the latest reports.

---

## Administrator Configuration Tasks

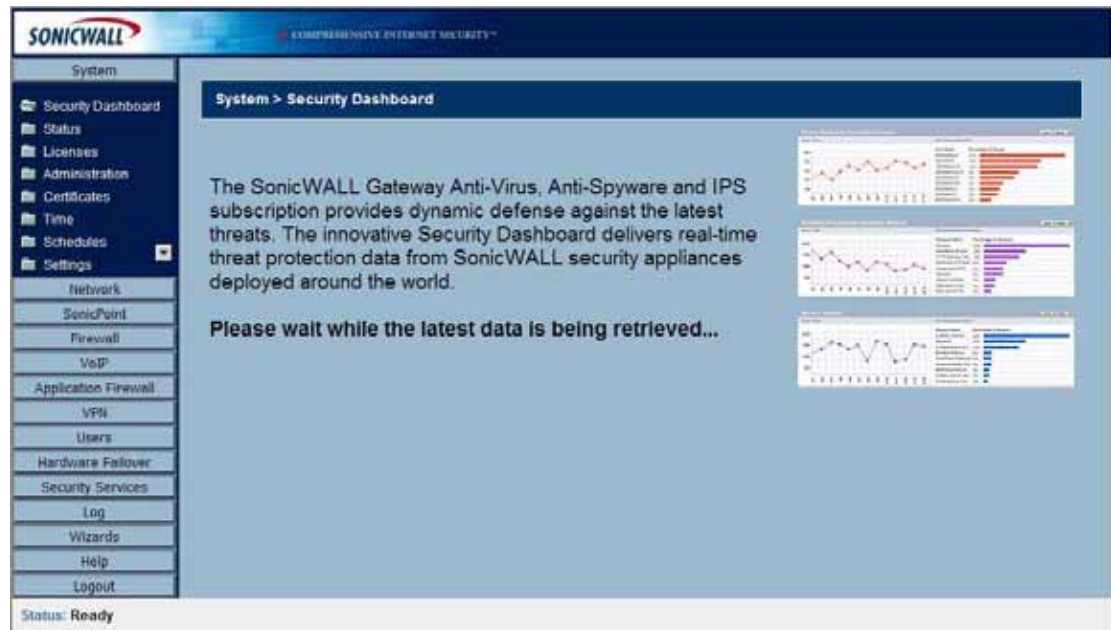
This section contains the following subsections:

- “SonicWALL Security Dashboard Configuration Overview” on page 51
- “Purchasing Security Services” on page 52

## SonicWALL Security Dashboard Configuration Overview

The SonicWALL Security Dashboard can be configured to display global or appliance-level statistics, to display statistics for different time periods, and to generate a custom PDF file. For information about purchasing SonicWALL security services that protect against the threats reported in the SonicWALL Security Dashboard, refer to “Purchasing Security Services” on page 52.

The SonicWALL Security Dashboard displays automatically upon successful login to a SonicWALL security appliance. You can access the SonicWALL Security Dashboard at any time by navigating to **System > Security Dashboard** in the left-hand menu. You may see the introductory screen shown below before the dashboard displays.



This section provides the following subsections:

- “Switching to Global or Appliance-Level View” on page 51
- “Selecting Custom Time Interval” on page 52
- “Generating a Security Dashboard PDF” on page 52

### Switching to Global or Appliance-Level View

To view SonicWALL Security Dashboard global reports, select the radio button next to **Global** in the top of the **System > Security Dashboard** screen. To view appliance-level reports, select the radio button next to the appliance serial number.

System > Security Dashboard >  Global  0006B1026C

### Selecting Custom Time Interval

The SonicWALL Security Dashboard reports default to a view of reports from the “Last 14 Days,” providing an aggregate view of threats blocked during that time period. You can configure each report to one of four optional time periods. Each report can be configured to reflect a different time period. To change a report to reflect a different time period, perform the following steps:

- Step 1** Select the report you want to change:
- Viruses Blocked by SonicWALL Network
  - Intrusions Prevented by SonicWALL Network
  - Spyware Blocked by SonicWALL Network
  - Multimedia (IM/P2P) Detected/Blocked by SonicWALL Network.
- Step 2** Next to the title of the selected report, click the pull-down menu and select one of the following options:
- **Last 12 Hours** - The selected report will display threat information from the last 12 hours
  - **Last 14 Days** - The selected report will display threat information from the last 14 days
  - **Last 21 Days** - The selected report will display threat information from the last 21 days
  - **Last 6 Months** - The selected report will display threat information from the last 6 months



### Generating a Security Dashboard PDF

To create a PDF version of the SonicWALL Security Dashboard, first select the desired view (global or appliance-level) and the desired time period for each report (the last 12 hours, 14 days, 21 days, or 6 months). Click the [Download PDF](#) button at the top of the page.

### Purchasing Security Services

To be protected from the threats reported in the SonicWALL Security Dashboard, it is recommended that you purchase SonicWALL security services. This section provides instructions for using the SonicWALL Registration & License Wizard, accessible from the SonicWALL appliance management interface, to purchase SonicWALL security services. SonicWALL security services include the following real-time protection services:

- **Gateway Anti-Virus** - Protects against viruses, worms, Trojans and other threats
- **Gateway Anti-Spyware** - Protects against new and existing malicious spyware
- **Intrusion Prevention Service** - Protects against application-layer attacks
- **Content Filtering Service** - Enhances protection and productivity by limiting access to objectionable Web content
- **Dynamic Support 8x5** - Provides one year of telephone and Web support, including software and firmware updates
- **ViewPoint** - Provides detailed and comprehensive reporting on network activity

**Note**

---

Your SonicWALL security appliance must be configured for Internet connectivity and must be connected to the Internet to use the Registration & License Wizard.

---

To purchase SonicWALL security services using the SonicWALL Registration & License Wizard, perform the following steps:

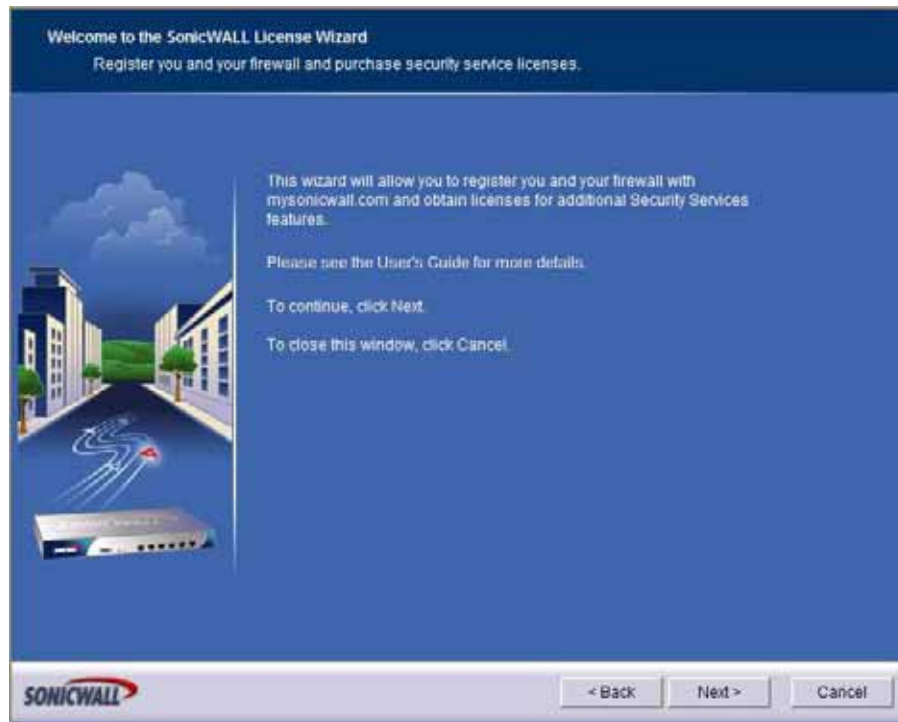
- Step 1** Log in to the SonicWALL appliance management interface.
- Step 2** In the left-navigation menu, click **Wizards**. The Configuration Wizard displays.



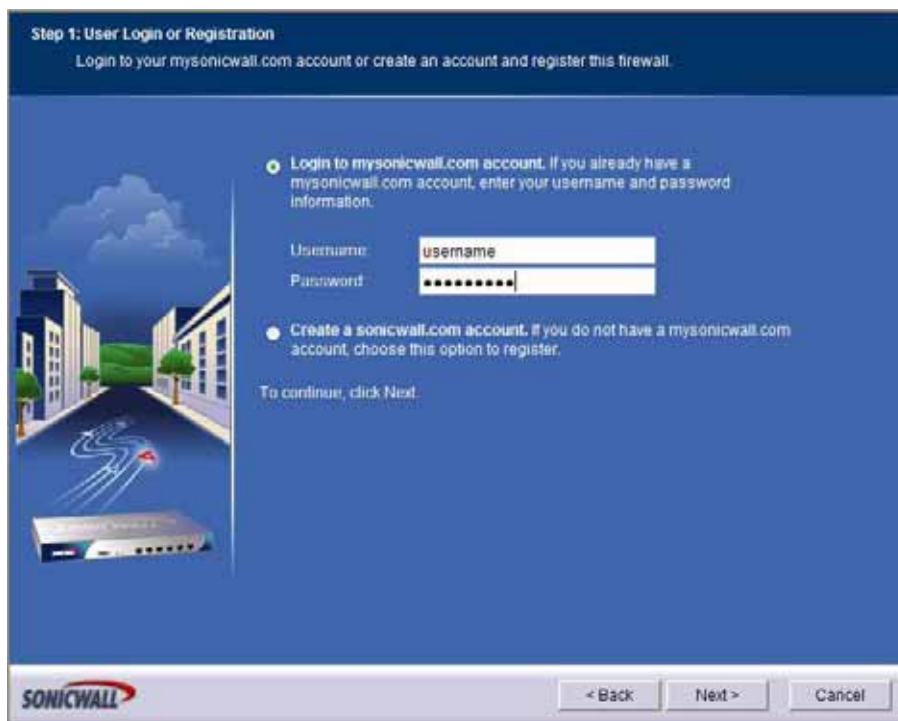
- Step 3** Select the radio button next to **Registration & License Wizard** and click **Next**.



- Step 4** The welcome screen displays. Click **Next**.



**Step 5** If you have a mysonicwall.com account, enter your username and password in the **Username** and **Password** fields. If you do not have a mysonicwall.com account, select the radio button next to **Create a sonicwall.com account**. Click **Next**.



**Step 6** If you selected **Create a sonicwall.com account**, the User Registration page displays. Provide the information requested in order to create your account, then click **Next**.



**Note**

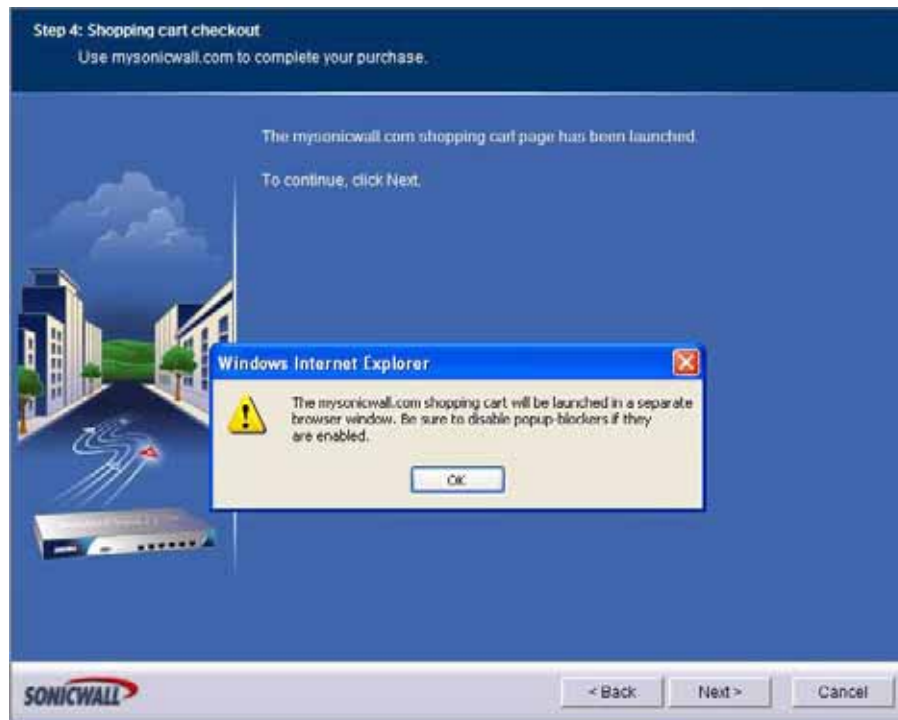
If you used an existing mysonicwall.com account by providing your username and password, you will not see this page. Skip to the next step.

**Step 7** Select the checkbox next to the service you want to purchase and click **Next**.

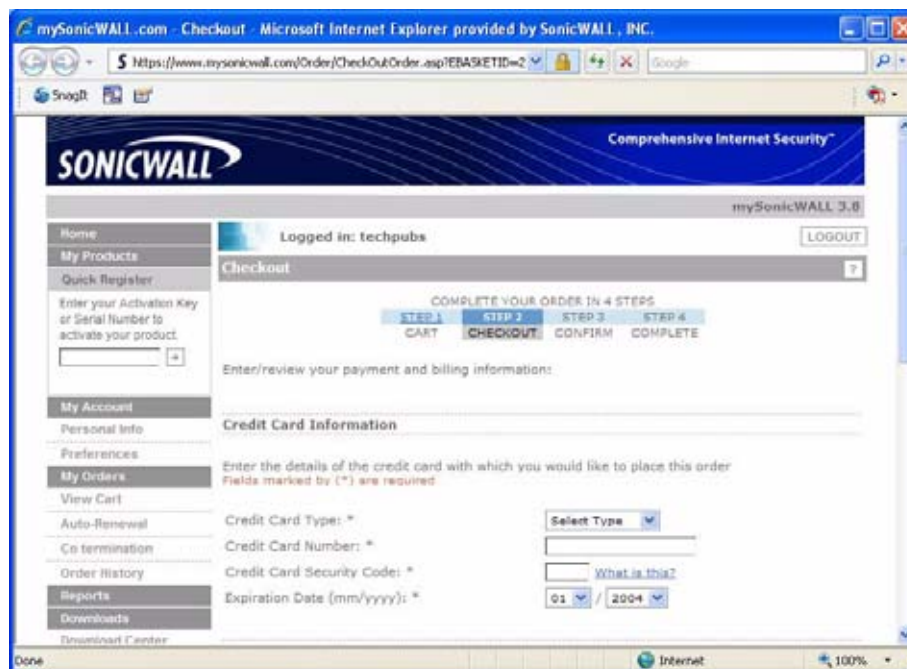
<input checked="" type="checkbox"/>	Part No.	Description	Unit Price
<input checked="" type="checkbox"/>	01-SSC-5851	SonicWALL Comprehensive Gateway Security Suite PRO 3060/4060	USD 3495.00
<input checked="" type="checkbox"/>	01-SSC-8821	Comprehensive Gateway Security Suite PRO 3060/4060 (2 Yrs)	USD 4241.00
<input checked="" type="checkbox"/>	01-SSC-8822	Comprehensive Gateway Security Suite PRO 3060/4060 (1 Yrs)	USD 5988.00

**Step 8** A notice displays that a separate browser window will be launched. Click **OK**.

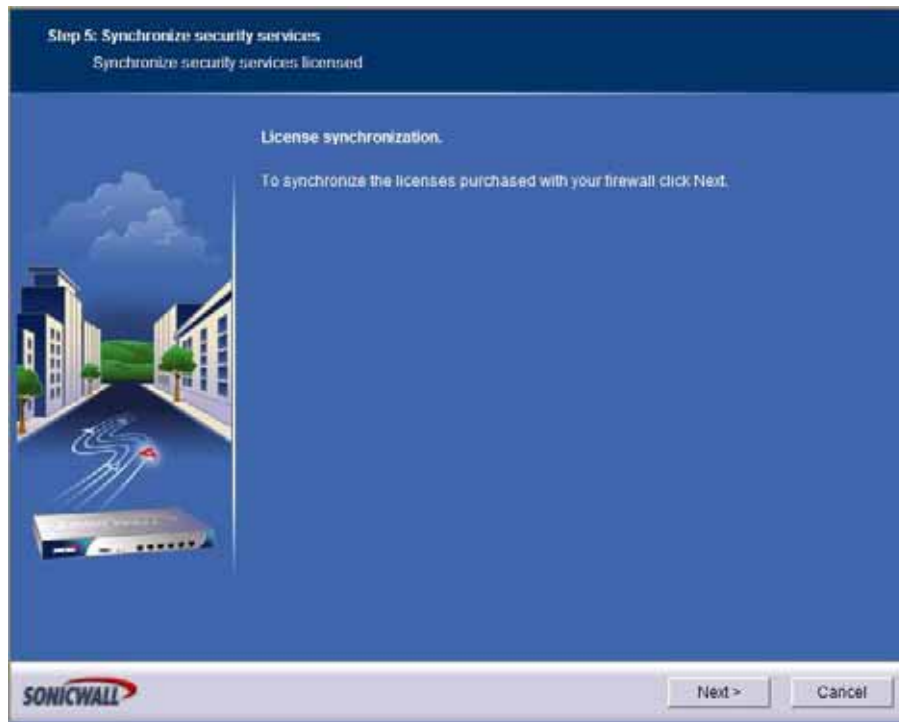




- Step 9** The mysonicwall.com page is launched in a separate browser window. Follow the on-screen instructions to complete the purchase of SonicWALL security services.



- Step 10** After you have purchased the security services, return to the wizard window. The License Synchronization window will synchronize the new security services with the SonicWALL security appliance. Click **Next** to complete the synchronization.



**Step 11** The Congratulations page displays. You have successfully purchased and synchronized your security services. Click **Close** to close the wizard.



To verify that the security services are licensed, navigate to **Security Services > Summary** in the left-hand menu and verify that the status of the services is **Licensed**. For information on advanced configuration for each service, refer to the SonicWALL *Administrator's Guides*, available on the Web at:

<http://www.sonicwall.com/us/Support.html>.

## Related Features

**SonicWALL Registration & License Wizard** - Use the SonicWALL Registration & License Wizard to purchase SonicWALL security services directly from your SonicWALL security appliance management interface.

**SonicWALL Security Services** - SonicWALL provides a comprehensive offering of security services that protect against the threats reported in the SonicWALL Security Dashboard. For a full list, visit the SonicWALL website at <http://www.sonicwall.com/us/Support.html>.

Some of the SonicWALL Security Services include:

- **Gateway Anti-Virus** - Protects against viruses, worms, Trojans and other threats
- **Gateway Anti-Spyware** - Protects against new and existing malicious spyware
- **Intrusion Prevention Service** - Protects against application-layer attacks
- **Content Filtering Service** - Enhances protection and productivity by limiting access to objectionable Web content
- **Dynamic Support 8x5** - Provides one year of telephone and Web support, including software and firmware updates
- **ViewPoint** - Provides detailed and comprehensive reporting on network activity



# CHAPTER 5

## Viewing Status Information

### System > Status

The **System > Status** page provides a comprehensive collection of information and links to help you manage your SonicWALL security appliance and SonicWALL Security Services licenses. It includes status information about your SonicWALL security appliance organized into five sections: **System Messages**, **System Information**, **Security Services**, **Latest Alerts**, and **Network Interfaces** as well as the **Wizards** button for accessing the **SonicWALL Configuration Wizard**.

The screenshot displays the 'System > Status' page with a 'Wizards...' button in the top right. The page is divided into several sections:

- System Messages:** Contains two red messages: 'Please check with SonicWALL for information about new Services and Upgrades for your Appliance.' and 'Log messages cannot be sent because you have not specified an outbound SMTP server address.'
- System Information:** A table listing hardware and software details:

Model:	PRO 2040 Enhanced
Serial Number:	0005B111A2C4
Authentication Code:	Y24Y-LJGH
Firmware Version:	SonicOS Enhanced 3.2.0.0-21e
ROM Version:	SonicROM 2.1.0.0
CPU (10s average):	0.50% - 800MHz VIA C3 Processor
Total Memory:	128MB RAM, 64MB Flash
System Time:	01/23/2006 17:21:50
Up Time:	2 Days 23:07:23
Current Connections:	344
Last Modified By:	192.168.168.65:30 01/22/2006 03:18:58
Registration Code:	HWE8WD8B
- Security Services:** A table showing the status of various services:

Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 20 Licenses (0 in use)
CFS (Content Filter)	Licensed
Network Anti-Virus	Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
E-Mail Filter	Licensed
ViewPoint	Licensed
- Latest Alerts:** A table listing recent alerts:

Date/Time	Message
01/23/2006 14:36:43	Possible port scan dropped
01/23/2006 13:54:09	Probable port scan dropped
01/23/2006 13:54:07	Possible port scan dropped
01/23/2006 12:20:24	Administrator login denied due to bad credentials
01/23/2006 10:50:49	Possible port scan dropped
- Network Interfaces:** A table showing interface details:

Name	IP Address	Link Status
X0 (LAN)	192.168.168.168	100 Mbps half-duplex
X1 (WAN)	68.35.78.194	100 Mbps full-duplex
X2 (WLAN)	172.16.31.1	100 Mbps full-duplex
X3 (LAN)	192.100.100.1	No Link

### Wizards

The **Wizards** button on the **System > Status** page provides access to the **SonicWALL Configuration Wizard**, which allows you to easily configure the SonicWALL security appliance using the following sub-wizards:

- **Setup Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to secure your Internet (WAN) and LAN connections.
- **Public Server Wizard** - This wizard helps you quickly configure the SonicWALL security appliance to provide public access to an internal server, such as a Web or E-mail server.
- **VPN Wizard** - This wizard helps you create a new site-to-site VPN Policy or configure the WAN GroupVPN to accept VPN connections from SonicWALL Global VPN Clients.
- **Wireless Wizard** - (SonicWALL TZ 170 Wireless and SonicWALL TZ 170 SP Wireless only), this wizard helps you select a wireless deployment mode and configure the radio settings of the built-in 802.11b/g antennas.

For more information on using the SonicWALL Configuration Wizard, see [“Wizards” on page 791](#).

## System Messages

Any information considered relating to possible problems with configurations on the SonicWALL security appliance such as password, log messages, as well as notifications of SonicWALL Security Services offers, new firmware notifications, and upcoming Security Service s expirations are displayed in the **System Messages** section.

## System Information

The following information is displayed in this section:

- **Model** - type of SonicWALL security appliance product
- **Serial Number** - also the MAC address of the SonicWALL security appliance
- **Authentication Code** - the alphanumeric code used to authenticate the SonicWALL security appliance on the registration database at <https://www.mysonicwall.com>.
- **Firmware Version** - the firmware version loaded on the SonicWALL security appliance.
- **ROM Version** - indicates the ROM version.
- **CPU** - displays the average CPU usage over the last 10 seconds and the type of the SonicWALL security appliance processor.
- **Total Memory** - indicates the amount of RAM and flash memory.
- **System Time** - The time registered on the internal clock on the SonicWALL appliance.
- **Up Time** - the length of time, in days, hours, and seconds the SonicWALL security appliance is active.
- **Current Connections** - the number of network connections currently existing on the SonicWALL security appliance.
- **Last Modified By** - The IP address of the user who last modified the system and the time stamp of the last modification.
- **Registration Code** - the registration code is generated when your SonicWALL security appliance is registered at <http://www.mysonicwall.com>.

## Latest Alerts

Any messages relating to system errors or attacks are displayed in this section. Attack messages include AV Alerts, forbidden e-mail attachments, fraudulent certificates, etc. System errors include WAN IP changed and encryption errors. Clicking the blue arrow displays the **Log > Log View** page.



Date/Time	Message
01/23/2006 14:36:43	Possible port scan dropped
01/23/2006 13:54:09	Probable port scan dropped
01/23/2006 13:54:07	Possible port scan dropped
01/23/2006 12:20:24	Administrator login denied due to bad credentials
01/23/2006 10:50:48	Possible port scan dropped

For more information on SonicWALL security appliance logging, see “[Log](#)” on page 763.

## Security Services

If your SonicWALL security appliance is not registered at mySonicWALL.com, the following message is displayed in the **Security Services** folder: **Your SonicWALL security appliance is not registered. Click [here](#) to Register your SonicWALL security appliance.** You need a mySonicWALL.com account to register your SonicWALL security appliance or activate security services. You can create a mySonicWALL.com account directly from the SonicWALL management interface.



If your SonicWALL security appliance is registered, a list of available SonicWALL Security Services are listed in this section with the status of **Licensed** or **Not Licensed**. If **Licensed**, the **Status** column displays the number of licenses and the number of licenses in use. Clicking the **Arrow** icon displays the **System > Licenses** page in the SonicWALL Web-based management interface. SonicWALL Security Services and SonicWALL security appliance registration is managed by mySonicWALL.com.



Service Name	Status
Nodes/Users	Licensed Unlimited Nodes
VPN	Licensed
Global VPN Client	Licensed - 20 Licenses (0 in use)
CFS (Content Filter)	Licensed
Network Anti-Virus	Licensed
Gateway Anti-Virus	Licensed
Anti-Spyware	Licensed
Intrusion Prevention	Licensed
E-Mail Filter	Licensed
ViewPoint	Licensed

Refer to [Part 13 Security Services](#) for more information on SonicWALL Security Services and activating them on the SonicWALL security appliance.

## Registering Your SonicWALL Security Appliance

Once you have established your Internet connection, it is recommended you register your SonicWALL security appliance. Registering your SonicWALL security appliance provides the following benefits:

- Try a FREE 30-day trial of SonicWALL Intrusion Prevention Service, SonicWALL Gateway Anti-Virus, Content Filtering Service, and Client Anti-Virus
- Activate SonicWALL security services and upgrades
- Access SonicOS firmware updates
- Get SonicWALL technical support

### Before You Register

If your SonicWALL security appliance is not registered, the following message is displayed in the **Security Services** folder on the **System > Status** page in the SonicWALL management interface: **Your SonicWALL is not registered. Click here to [Register your SonicWALL](#).** You need a mySonicWALL.com account to register the SonicWALL security appliance.

If your SonicWALL security appliance is connected to the Internet, you can create a mySonicWALL.com account and register your SonicWALL security appliance directly from the SonicWALL management interface. If you already have a mySonicWALL.com account, you can register the SonicWALL security appliance directly from the management interface.

Your mySonicWALL.com account is accessible from any Internet connection by pointing your Web browser to <https://www.mysonicwall.com>. mySonicWALL.com uses the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information.

**Note**

Make sure the **Time Zone** and **DNS** settings on your SonicWALL security appliance are correct when you register the device. See SonicWALL Setup Wizard instructions for instructions on using the **Setup Wizard** to set the **Time Zone** and **DNS** settings.

**Note**

mySonicWALL.com registration information is not sold or shared with any other company.

You can also register your security appliance at the <https://www.mysonicwall.com> site by using the **Serial Number** and **Authentication Code** displayed in the **Security Services** section. Click the **SonicWALL** link to access your mySonicWALL.com account. You will be given a registration code after you have registered your security appliance. Enter the registration code in the field below the **You will be given a registration code, which you should enter below** heading, then click **Update**.

### Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL management interface.



To create a mySonicWALL.com account from the SonicWALL management interface:

- Step 1** In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



- Step 2** Click the **here** link in **If you do not have a mySonicWALL account, please click here to create one** on the **mySonicWALL Login** page.



- Step 3** In the **MySonicWALL Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields in the mySonicWALL.com account form. All fields marked with an \* are required fields.



**Note** Remember your username and password to access your mySonicWALL.com account.

- Step 4** Click **Submit** after completing the **MySonicWALL Account** form.
- Step 5** When the mySonicWALL.com server has finished processing your account, a page is displayed confirming your account has been created. Click **Continue**.
- Step 6** Congratulations! Your mySonicWALL.com account is activated. Now you need to log into mySonicWALL.com from the management appliance to register your SonicWALL security appliance.

## Registering Your SonicWALL Security Appliance

If you already have a mySonicWALL.com account, follow these steps to register your security appliance:

- Step 1** In the **Security Services** section on the **System > Status** page, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL**. The **mySonicWALL Login** page is displayed.



- Step 2** In the **mySonicWALL.com Login** page, enter your mySonicWALL.com username and password in the **User Name** and **Password** fields and click **Submit**.
- Step 3** The next several pages inform you about free trials available to you for SonicWALL's Security Services:
- **Gateway Anti-Virus** - protects your entire network from viruses
  - **Client Anti-Virus** - protects computers on your network from viruses
  - **Premium Content Filtering Service** - protects your network and improves productivity by limiting access to unproductive and inappropriate Web sites
  - **Intrusion Prevention Service** - protects your network from Trojans, worms, and application layer attacks
- Step 4** Click **Continue** on each page.
- Step 5** At the top of the Product Survey page, enter a friendly name for your SonicWALL security appliance in the **Friendly name** field, and complete the optional product survey.
- Step 6** Click **Submit**.
- Step 7** When the mySonicWALL.com server has finished processing your registration, a page is displayed confirming your SonicWALL security appliance is registered.
- Step 8** Click **Continue**. The **Manage Services Online** table on the **System > Licenses** page displayed.

## Network Interfaces

**Network Interfaces** displays information about the interfaces for your SonicWALL security appliance. Clicking the blue arrow displays the **Network > Interfaces** page for configuring your **Network** settings. The available interfaces displayed in the Network Interfaces section depend on the SonicWALL security appliance model.

# CHAPTER 6

## Managing SonicWALL Licenses

### System > Licenses

The **System > Licenses** page provides links to activate, upgrade, or renew SonicWALL Security Services licenses. From this page in the SonicWALL Management Interface, you can manage all the SonicWALL Security Services licensed for your SonicWALL security appliance. The information listed in the **Security Services Summary** table is updated from your mySonicWALL.com account. The **System > Licenses** page also includes links to FREE trials of SonicWALL Security Services.

### Node License Status

A node is a computer or other device connected to your LAN with an IP address.

If your SonicWALL security appliance is licensed for unlimited nodes, the **Node License Status** section displays the message: **The SonicWALL is licensed for unlimited Nodes/Users**. No other settings are displayed.

If your SonicWALL security appliance is not licensed for unlimited nodes, the **Node License Status** table lists how many nodes your security appliance is licensed to have connected at any one time, how many nodes are currently connected, and how many nodes you have in your **Node License Exclusion List**.




The **Currently Licensed Nodes** table lists details on each node connected to your security appliance.

MAC Address	IP Address	Interface	Name	Exclude
00:0e:56:e5:35:7c	192.168.168.1	LAN	FWA	<input type="checkbox"/>

## Excluding a Node

When you exclude a node, you block it from connecting to your network through the security appliance. Excluding a node creates an address object for that IP address and assigns it to the Node License Exclusion List address group.

To exclude a node:

- Step 1** Select the node you want to exclude in the **Currently Licensed Nodes** table on the **System > Licenses** page, and click the  icon in the **Exclude** column for that node.
- Step 2** A warning displays, saying that excluding this node will create an address object for it and place it in the **License Exclusion List** address group. Click **OK** to exclude the node.

You can manage the **License Exclusion List** group and address objects in the **Network > Address Objects** page of the management interface. Click the **Node License Exclusion List** link to jump to the **Network > Address Objects** page. See **Chapter 19, Network > Address Objects** for instructions on managing address objects.

## Security Services Summary

The **Security Services Summary** table lists the available and activated security services on the SonicWALL security appliance.

Security Service	Status	Count	Expiration
Nodes/Users	Licensed	Unlimited	
Network Anti-Virus	Expired	100	
Intrusion Prevention Service	Expired		
Gateway AntiVirus	Not Licensed		
Server Anti-Virus	Not Licensed		
CFP Standard	Expired		
Premium Content Filtering Service	Free Trial		06 May 2005
E-Mail Filtering Service	Not Licensed		
VPN	Licensed		
Global VPN Client	Not Licensed		
Global VPN Client Enterprise	Licensed	2000	
SonicOS Enhanced	Licensed		
Global Security Client	Not Licensed		
ViewPoint	Licensed		

The **Security Service** column lists all the available SonicWALL Security Services and upgrades available for the SonicWALL security appliance. The **Status** column indicates is the security service is activated (**Licensed**), available for activation (**Not Licensed**), or no longer active (**Expired**). The number of nodes/users allowed for the license is displayed in the **Count** column. The **Expiration** column displays the expiration date for any Licensed Security Service.

The information listed in the **Security Services Summary** table is updated from your mySonicWALL.com account the next time the SonicWALL security appliance automatically synchronizes with your mySonicWALL.com account (once a day) or you can click the link in **To synchronize licenses with mySonicWALL.com click here** in the **Manage Security Services Online** section.

For more information on SonicWALL Security Services, see [“Security Services” on page 685](#).

## Manage Security Services Online

To activate, upgrade, or renew services, click the link in **To Activate, Upgrade, or Renew services, click here**. Click the link in **To synchronize licenses with mySonicWALL.com click here** to synchronize your mySonicWALL.com account with the **Security Services Summary** table.



You can also get free trial subscriptions to SonicWALL Content Filter Service and Client Anti-Virus by clicking the **For Free Trials click here** link. When you click these links, the **mySonicWALL.com Login** page is displayed.

Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields and click **Submit**. The **Manage Services Online** page is displayed with licensing information from your mySonicWALL.com account.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	100	04 Aug 2004
Intrusion Prevention Service	Expired		Renew		06 Jun 2004
Gateway AntiVirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
CFS Standard	Expired		Renew		05 Jun 2004
CFS Premium Service	Free Trial		Renew		06 May 2005
E-Mail Filtering Service	Not Licensed				
VPN	Licensed				
Global VPN Client	Not Licensed		Activate		
Global VPN Client Enterprise	Licensed		Upgrade Share	2000	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Licensed				

## Manual Upgrade

**Manual Upgrade** allows you to activate your services by typing the service activation key supplied with the service subscription not activated on mySonicWALL.com. Type the activation key from the product into the **Enter upgrade key** field and click **Submit**.

## Manual Upgrade for Closed Environments

If your SonicWALL security appliance is deployed in a high security environment that does not allow direct Internet connectivity from the SonicWALL security appliance, you can enter the encrypted license key information from <http://www.mysonicwall.com> manually on the **System > Licenses** page in the SonicWALL Management Interface.



### Note

Manual upgrade of the encrypted License Keyset is only for Closed Environments. If your SonicWALL security appliance is connected to the Internet, it is recommended you use the automatic registration and Security Services upgrade features of your SonicWALL security appliance.

## From a Computer Connected to the Internet

- Step 1** Make sure you have an account at <http://www.mysonicwall.com> and your SonicWALL security appliance is registered to the account before proceeding.
- Step 2** After logging into [www.mysonicwall.com](http://www.mysonicwall.com), click on your registered SonicWALL security appliance listed in **Registered SonicWALL Products**.
- Step 3** Click the **View License Keyset** link. The scrambled text displayed in the text box is the License Keyset for the selected SonicWALL security appliance and activated Security Services. Copy the Keyset text for pasting into the **System > Licenses** page or print the page if you plan to manually type in the Keyset into the SonicWALL security appliance.

## From the Management Interface of your SonicWALL Security Appliance

---

- Step 1** Make sure your SonicWALL security appliance is running SonicOS Standard or Enhanced 2.1 (or higher).
- Step 2** Paste (or type) the Keyset (from the step 3) into the Keyset field in the **Manual Upgrade** section of the **System > Licenses** page (SonicOS).
- Step 3** Click the **Submit** or the **Apply** button to update your SonicWALL security appliance. The status field at the bottom of the page displays The configuration has been updated.
- Step 4** You can generate the **System > Diagnostics > Tech Support Report** to verify the upgrade details.



**Note** After the manual upgrade, the **System > Licenses** page does not contain any registration and upgrade information.

---

**Caution** The warning message: **SonicWALL Registration Update Needed. Please update your registration information** remains on the **System > Status** page after you have registered your SonicWALL security appliance. Ignore this message.

---







## CHAPTER 7

# Configuring Administration Settings

---

## System > Administration

The System Administration page provides settings for the configuration of SonicWALL security appliance for secure and remote management. You can manage the SonicWALL using a variety of methods, including HTTPS, SNMP or SonicWALL Global Management System (SonicWALL GMS). This chapter contains the following sections:

- [“Firewall Name” on page 73](#)
- [“Administrator Name & Password” on page 73](#)
- [“Login Security Settings” on page 74](#)
- [“Multiple Administrators” on page 76](#)
- [“Web Management Settings” on page 77](#)
- [“SSH Management Settings” on page 78](#)
- [“Advanced Management” on page 78](#)
- [“Download URL” on page 82](#)
- [“Selecting UI Language” on page 83](#)

### Firewall Name

The **Firewall Name** uniquely identifies the SonicWALL security appliance and defaults to the serial number of the SonicWALL. The serial number is also the MAC address of the unit. To change the **Firewall Name**, type a unique alphanumeric name in the **Firewall Name** field. It must be at least 8 characters in length.

### Administrator Name & Password

The **Administrator Name** can be changed from the default setting of **admin** to any word using alphanumeric characters up to 32 characters in length. To create a new administrator name, type the new name in the **Administrator Name** field. Click **Apply** for the changes to take effect on the SonicWALL.

## Changing the Administrator Password

To set a new password for SonicWALL Management Interface access, type the old password in the **Old Password** field, and the new password in the **New Password** field. Type the new password again in the **Confirm New Password** field and click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.



**Tip**

It's recommended you change the default password "**password**" to your own custom password.

## Login Security Settings

The internal SonicWALL web-server now only supports SSL version 3.0 and TLS with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128 bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 roll-back vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.



**Tip**

By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL recommends using these most recent web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0. In Internet Explorer, go to **Tools > Internet Options**, click on the **Advanced** tab, and scroll to the bottom of the **Settings** menu. In Firefox, go to **Tools > Options**, click on the **Advanced** tab, and then click on the **Encryption** tab.

The screenshot shows the 'Login Security' configuration page. It includes the following settings:

- Password must be changed every (days): 90
- Bar repeated passwords for this many changes: 4
- Enforce a minimum password length of: 1
- Enforce password complexity: Require alphabetic, numeric and symbolic characters
- Apply these password constraints for:
  - Administrator
  - Other full administrators
  - Limited administrators
  - Other local users
- Log out the administrator after inactivity of (minutes): 55
- Enable administrator/user lockout
  - Failed login attempts per minute before lockout: 5
  - Lockout Period (minutes): 5

SonicOS Enhanced 4.0 introduces password constraint enforcement, which can be configured to ensure that administrators and users are using secure passwords. This password constraint enforcement can satisfy the confidentiality requirements as defined by current information security management systems or compliance requirements, such as Common Criteria and the Payment Card Industry (PCI) standard.

The **Password must be changed every (days)** setting requires users to change their passwords after the designated number of days has elapsed. When a user attempts to login with an expired password, a pop-up window will prompt the user to enter a new password. The **User Login Status** window now includes a **Change Password** button so that users can change their passwords at any time.

The **Bar repeated passwords for this many changes** setting requires users to use unique passwords for the specified number of password changes.

The **Enforce a minimum password length of** setting sets the shortest allowed password.

The **Enforce password complexity** pulldown menu provides the following options:

- Require both alphabetic and numeric characters
- Require alphabetic, numeric, and symbolic characters

The **Apply these password constraints for** checkboxes specify which classes of users the password constraints are applied to. The **administrator** checkbox refers to the default administrator with the username **admin**.

The **Log out the Administrator Inactivity Timeout after inactivity of (minutes)** setting allows you to set the length of inactivity time that elapses before you are automatically logged out of the Management Interface. By default, the SonicWALL security appliance logs out the administrator after 5 minutes of inactivity. The inactivity timeout can range from 1 to 99 minutes. Click **Apply**, and a message confirming the update is displayed at the bottom of the browser window.



**Tip**

If the Administrator Inactivity Timeout is extended beyond 5 minutes, you should end every management session by clicking Logout to prevent unauthorized access to the SonicWALL security appliance's Management Interface.

You can configure the SonicWALL security appliance to lockout an administrator or a user if the login credentials are incorrect. Select the **Enable Administrator/User Lockout on login failure** checkbox to prevent users from attempting to log into the SonicWALL security appliance without proper authentication credentials. Type the number of failed attempts before the user is locked out in the **Failed login attempts per minute before lockout** field. Type the length of time that must elapse before the user attempts to log into the SonicWALL again in the **Lockout Period (minutes)** field.

**Caution**

If the administrator and a user are logging into the SonicWALL using the same source IP address, the administrator is also locked out of the SonicWALL. The lockout is based on the source IP address of the user or administrator.

## Multiple Administrators

SonicOS Enhanced provides the ability for multiple administrators to access the SonicOS Management Interface simultaneously. For more information on Multiple Administrators, see the “[Multiple Administrator Support Overview](#)” section on page 590. The **System > Administration** page contains a number of options to manage multiple administrators.

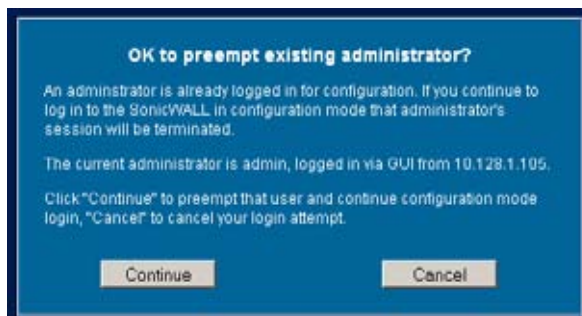


- The **On preemption by another administrator** setting configures what happens when one administrator preempts another administrator using the Multiple Administrators feature. The preempted administrator can either be converted to non-config mode or logged out.
  - **Drop to non-config mode** - Select to allow more than one administrator to access the appliance in non-config mode without disrupting the current administrator.
  - **Log Out** - Select to have the new administrator preempt the current administrator.
- **Allow preemption by a lower priority administrator after inactivity of (minutes)** - Enter the number of minutes of inactivity by the current administrator that will allow a lower-priority administrator to preempt.
- **Enable inter-administrator messaging** - Select to allow administrators to send text messages through the management interface to other administrators logged into the appliance. The message will appear in the browser’s status bar.
- **Messaging polling interval** - Sets how often the administrator’s browser will check for inter-administrator messages. If there are likely to be multiple administrators who need to access the appliance, this should be set to a reasonably short interval to ensure timely delivery of messages.

## Activating Configuration Mode

You can switch between configuration mode and non-config mode by clicking the button in the Web Management section (directly below the Multiple Administrator section).

When you are in configuration mode, the **End. config mode** button is displayed. When you are in configuration mode, the **Configuration mode** button is displayed. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode. If another administrator is in configuration mode, the following message displays.



Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

## Web Management Settings

The SonicWALL security appliance can be managed using HTTP or HTTPS and a Web browser. Both HTTP and HTTPS are enabled by default. The default port for HTTP is port 80, but you can configure access through another port. Type the number of the desired port in the **Port** field, and click **Apply**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the SonicWALL security appliance. For example, if you configure the port to be 76, then you must type <LAN IP Address>:76 into the Web browser, i.e. <http://192.168.168.1:76>. The default port for HTTPS management is **443**.

You can add another layer of security for logging into the SonicWALL security appliance by changing the default port. To configure another port for HTTPS management, type the preferred port number into the **Port** field, and click **Update**. For example, if you configure the HTTPS Management Port to be 700, then you must log into the SonicWALL using the port number as well as the IP address, for example, <https://192.168.168.1:700> to access the SonicWALL.

The **Certificate Selection** menu allows you to use a self-signed certificate (**Use Self-signed Certificate**), which allows you to continue using a certificate without downloading a new one each time you log into the SonicWALL security appliance. You can also choose **Import Certificate** to select an imported certificate from the **System > Certificates** page to use for authentication to the management interface.

When the **Use System Dashboard View as starting page** checkbox is enabled, the **System > Dashboard** page will be displayed when you first log into the SonicWALL security appliance. If this option is disabled, the **System > Status** page will be displayed.

The **Delete Cookies** button removes all browser cookies saved by the SonicWALL appliance. Deleting cookies will cause you to lose any unsaved changes made in the Management interface.

## Changing the Default Size for SonicWALL Management Interface Tables

The SonicWALL Management Interface allows you to control the display of large tables of information across all tables in the management Interface. You can change the default table page size in all tables displayed in the SonicWALL Management Interface from the default 50 items per page to any size ranging from 1 to 5,000 items.

To change the default table size:

- 
- Step 1** Enter the maximum table size number in the **Table Size** field.
  - Step 2** Click **Apply**.

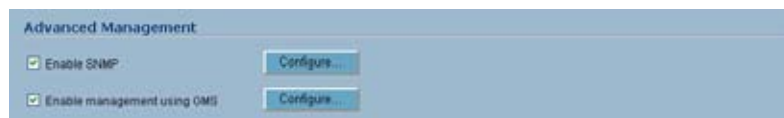
## SSH Management Settings



If you use SSH to manage the SonicWALL appliance, you can change the SSH port for additional security. The default SSH port is **22**.

## Advanced Management

You can manage the SonicWALL security appliance using SNMP or SonicWALL Global Management System. The following sections explain how to configure the SonicWALL for management by these two options.



For more information on SonicWALL Global Management System, go to <http://www.sonicwall.com>.

## Enabling SNMP Management

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SonicWALL security appliance and receive notification of critical events as they occur on the network. The SonicWALL security appliance supports SNMP v1/v2c and all relevant Management Information Base II (MIB) groups except **egp** and **at**. The SonicWALL security appliance replies to SNMP Get commands for MIBII via any interface and supports a custom SonicWALL MIB for generating trap messages. The custom SonicWALL MIB is available for download from the SonicWALL Web site and can be loaded into third-party SNMP management software such as HP Openview, Tivoli, or SNMPC.

To enable SNMP on the SonicWALL security appliance, log into the Management interface and click **System**, then Administration. Select the **Enable SNMP** checkbox, and then click **Configure**. The **Configure SNMP** window is displayed.

- Step 1** Type the host name of the SonicWALL security appliance in the **System Name** field.
- Step 2** Type the network administrator's name in the **System Contact** field.
- Step 3** Type an e-mail address, telephone number, or pager number in the **System Location** field.
- Step 4** Type a name for a group or community of administrators who can view SNMP data in the **Get Community Name** field.
- Step 5** Type a name for a group or community of administrators who can view SNMP traps in the **Trap Community Name** field.
- Step 6** Type the IP address or host name of the SNMP management system receiving SNMP traps in the Host 1 through Host 4 fields. You must configure at least one IP address or host name, but up to four addresses or host names can be used.
- Step 7** Click **OK**.

### Configuring Log/Log Settings for SNMP

Trap messages are generated only for the alert message categories normally sent by the SonicWALL security appliance. For example, attacks, system errors, or blocked Web sites generate trap messages. If none of the categories are selected on the **Log > Settings** page, then no trap messages are generated.

### Configuring SNMP as a Service and Adding Rules

By default, SNMP is disabled on the SonicWALL security appliance. To enable SNMP you must first enable SNMP on the **System > Administration** page, and then enable it for individual interfaces. To do this, go to the **Network > Interfaces** page and click on the **Configure** button for the interface you want to enable SNMP on.

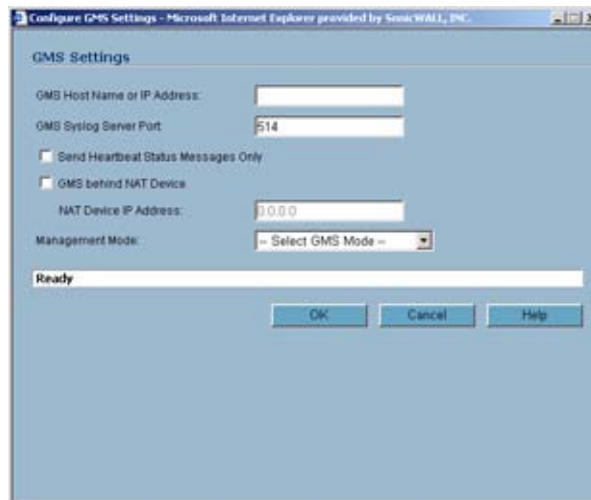
For instructions on adding services and rules to the SonicWALL security appliance, see Part 5 Firewall.

If your SNMP management system supports discovery, the SonicWALL security appliance agent automatically discover the SonicWALL security appliance on the network. Otherwise, you must add the SonicWALL security appliance to the list of SNMP-managed devices on the SNMP management system.

## Enable GMS Management

You can configure the SonicWALL security appliance to be managed by SonicWALL Global Management System (SonicWALL GMS). To configure the SonicWALL security appliance for GMS management:

- Step 1** Select the **Enable Management using GMS** checkbox, then click **Configure**. The **Configure GMS Settings** window is displayed.



- Step 2** Enter the host name or IP address of the GMS Console in the **GMS Host Name or IP Address** field.
- Step 3** Enter the port in the **GMS Syslog Server Port** field. The default value is **514**.
- Step 4** Select **Send Heartbeat Status Messages Only** to send only heartbeat status instead of log messages.
- Step 5** Select **GMS behind NAT Device** if the GMS Console is placed behind a device using NAT on the network. Type the IP address of the NAT device in the **NAT Device IP Address** field.
- Step 6** Select one of the following GMS modes from the Management Mode menu.
- **IPSEC Management Tunnel** - Selecting this option allows the SonicWALL security appliance to be managed over an IPsec VPN tunnel to the GMS management console. The default IPsec VPN settings are displayed. Select **GMS behind NAT Device** if applicable to



the GMS installation, and enter the IP address in the **NAT Device IP Address** field. The default VPN policy settings are displayed at the bottom of the **Configure GMS Settings** window.

Configure GMS Settings - Microsoft Internet Explorer provided by SonicWALL, INC.

GMS Settings

GMS Host Name or IP Address:

GMS Syslog Server Port:

Send Heartbeat Status Messages Only

GMS behind NAT Device

NAT Device IP Address:

Management Mode:

Inbound/Outbound SPI:

Encryption Algorithms:

Encryption Key:

Authentication Key:

Ready

OK Cancel Help

- **Existing Tunnel** - If this option is selected, the GMS server and the SonicWALL security appliance already have an existing VPN tunnel over the connection. Enter the GMS host name or IP address in the **GMS Host Name or IP Address** field. Enter the port number in the **Syslog Server Port** field.

Configure GMS Settings - Microsoft Internet Explorer provided by SonicWALL, INC.

GMS Settings

GMS Host Name or IP Address:

GMS Syslog Server Port:

Send Heartbeat Status Messages Only

GMS behind NAT Device

NAT Device IP Address:

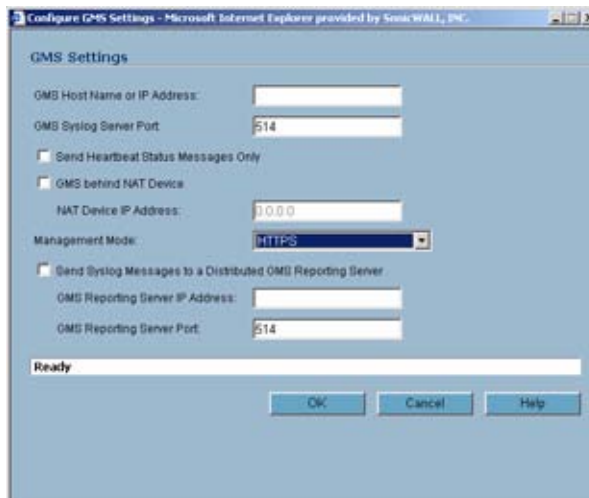
Management Mode:

Note: The existing established tunnel will be used.

Ready

OK Cancel Help

- **HTTPS** - If this option is selected, HTTPS management is allowed from two IP addresses: the GMS Primary Agent and the Standby Agent IP address. The SonicWALL security appliance also sends encrypted syslog packets and SNMP traps using 3DES and the SonicWALL security appliance administrator's password. The following configuration settings for HTTPS management mode are displayed:



- **Send Syslog Messages in Cleartext Format** - Sends heartbeat messages as cleartext.
- **Send Syslog Messages to a Distributed GMS Reporting Server** - Sends regular heartbeat messages to both the GMS Primary and Standby Agent IP address. The regular heartbeat messages are sent to the specified GMS reporting server and the reporting server port.
- **GMS Reporting Server IP Address** - Enter the IP address of the GMS Reporting Server, if the server is separate from the GMS management server.
- **GMS Reporting Server Port** - Enter the port for the GMS Reporting Server. The default value is 514

Step 7 Click **OK**.

## Download URL

SonicWALL Global VPN Client (GVC) and SonicWALL Global Security Client (GSC) allow users to connect securely to your network using the GroupVPN Policy on the port they are connecting to. GVC or the VPN client portion of GSC is required for a user to connect to the GroupVPN Policy. Depending on how you have set up your VPN policies, if a user does not have the latest GVC or GSC software installed, the user will be directed to a URL to download the latest GVC or GSC software.

The **Download URL** section provides a field for entering the URL address of a site for downloading the SonicWALL Global VPN Client application, when a user is prompted to use the Global VPN Client for access to the network.



The default URL <http://help.mysonicwall.com/applications/vpnclient> displays the SonicWALL Global VPN Client download site. You can point to any URL where you provide the SonicWALL Global VPN Client application.

## Selecting UI Language

If your firmware contains other languages besides English, they can be selected in the **Language Selection** pulldown menu.

**Note**

---

Changing the language of the SonicOS UI requires that the SonicWALL security appliance be rebooted.

---





## CHAPTER 8

# Managing Certificates

---

## System > Certificates

To implement the use of certificates for VPN policies, you must locate a source for a valid CA certificate from a third party CA service. Once you have a valid CA certificate, you can import it into the SonicWALL security appliance to validate your Local Certificates. You import the valid CA certificate into the SonicWALL security appliance using the **System > Certificates** page. Once you import the valid CA certificate, you can use it to validate your local certificates.

## Digital Certificates Overview

A digital certificate is an electronic means to verify identity by a trusted third party known as a Certificate Authority (CA). The X.509 v3 certificate standard is a specification to be used with cryptographic certificates and allows you to define extensions which you can include with your certificate. SonicWALL has implemented this standard in its third party certificate support.

You can use a certificate signed and verified by a third party CA to use with an IKE (Internet Key Exchange) VPN policy. IKE is an important part of IPsec VPN solutions, and it can use digital certificates to authenticate peer devices before setting up SAs. Without digital certificates, VPN users must authenticate by manually exchanging shared secrets or symmetric keys. Devices or clients using digital signatures do not require configuration changes every time a new device or client is added to the network.

A typical certificate consists of two sections: a data section and a signature section. The data section typically contains information such as the version of X.509 supported by the certificate, a certificate serial number, information, information about the user's public key, the Distinguished Name (DN), validation period for the certificate, optional information such as the target use of the certificate. The signature section includes the cryptographic algorithm used by the issuing CA, and the CA digital signature.

SonicWALL security appliances interoperate with any X.509v3-compliant provider of Certificates. SonicWALL security appliances have been tested with the following vendors of Certificate Authority Certificates:

- Entrust
- Microsoft
- OpenCA

- OpenSSL
- VeriSign

#	Certificate	Type	Validated	Expires	Details	Configure
1	HTTPS Management Certificate	Local certificate	Self-signed	Jan 19 03:14:07 2018 OMT		
2	Thawte Server	CA certificate		Dec 31 23:59:59 2020 OMT		
3	Thawte Premium Server	CA certificate		Dec 31 23:59:59 2020 OMT		
4	VeriSign RSA Secure Server	CA certificate		Jan 7 23:59:59 2010 OMT		
5	VeriSign Class 3 Public Primary	CA certificate		Aug 1 23:59:59 2028 OMT		
6	Equifax Secure	CA certificate		Aug 22 16:41:51 2018 OMT		
7	Equifax Secure Global eBusiness	CA certificate		Jun 21 04:00:00 2020 OMT		
8	SonicWALL Root CA	CA certificate		May 10 23:59:59 2010 OMT		
9	SonicWALL CA	CA certificate		May 10 23:59:59 2005 OMT		




## Certificates and Certificate Requests


The **Certificate and Certificate Requests** section provides all the settings for managing CA and Local Certificates.

The **View Style** menu allows you to display your certificates in the **Certificates and Certificate Requests** table based on the following criteria:

- **All Certificates** - displays all certificates and certificate requests.
- **Imported certificates and requests** - displays all imported certificates and generated certificate requests.
- **Built-in certificates** - displays all certificates included with the SonicWALL security appliance.
- **Include expired and built-in certificates** - displays all expired and built-in certificates.

The **Certificates and Certificate Requests** table displays the following information about your certificates:

- **Certificate** - the name of the certificate.
- **Type** - the type of certificate, which can include CA or Local.
- **Validated** - the validation information.
- **Expires** - the date and time the certificate expires.
- **Details** - the details of the certificate. Moving the pointer over the  icon displays the details of the certificate.
- **Configure** - Displays the  edit and delete  icons for editing or deleting a certificate entry

Also displays the Import icon  to import either certificate revocation lists (for CA certificates) or signed certificates (for Pending requests).

## Certificate Details

Clicking on the icon in the **Details** column of the **Certificates and Certificate Requests** table lists information about the certificate, which may include the following, depending on the type of certificate:

- Certificate Issuer
- Subject Distinguished Name
- Certificate Serial Number
- Valid from
- Expires On
- Status (for Pending requests and local certificates)
- CRL Status (for Certificate Authority certificates)

The details shown in the **Details** mouseover popup depend on the type of certificate. **Certificate Issuer**, **Certificate Serial Number**, **Valid from**, and **Expires On** are not shown for Pending requests since this information is generated by the Certificate provider. Similarly, **CRL Status** information is shown only for CA certificates and varies depending on the CA certificate configuration.

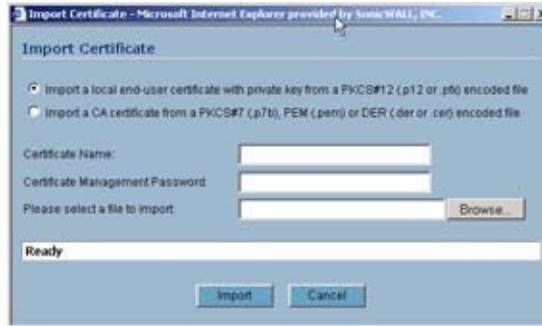
## Importing Certificates

After your CA service has issued a Certificate for your Pending request, or has otherwise provided a Local Certificate, you can import it for use in VPN or Web Management authentication. CA Certificates may also be imported to verify local Certificates and peer Certificates used in IKE negotiation.

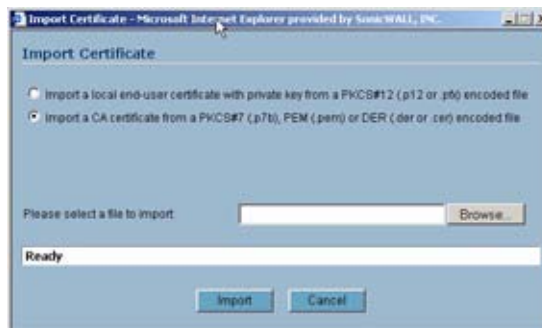
## Importing a Certificate Authority Certificate


To import a certificate from a certificate authority, perform these steps:

- Step 1** Click **Import**. The **Import Certificate** window is displayed.



- Step 1** Select **Import a CA certificate from a PKCS#7 (\*.p7b) or DER (.der or .cer) encoded file**. The **Import Certificate** window settings change.



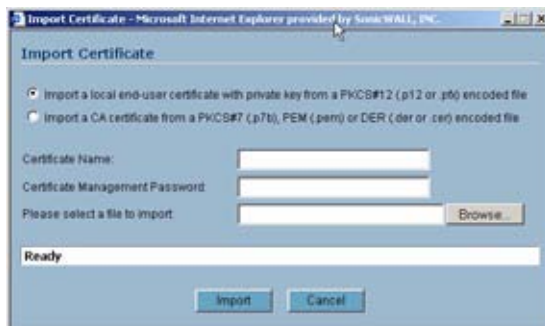
- Step 2** Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.
- Step 3** Click **Import** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.
- Step 4** Moving your pointer to the  icon in the **Details** column displays the certificate details information.




## Importing a Local Certificate

To import a local certificate, perform these steps:

- Step 1** Click **Import**. The **Import Certificate** window is displayed.



- Step 2** Enter a certificate name in the **Certificate Name** field.
- Step 3** Enter the password used by your Certificate Authority to encrypt the PKCS#12 file in the **Certificate Management Password** field.
- Step 4** Enter the path to the certificate file in the **Please select a file to import** field or click **Browse** to locate the certificate file, and then click **Open** to set the directory path to the certificate.
- Step 5** Click **Import** to import the certificate into the SonicWALL security appliance. Once it is imported, you can view the certificate entry in the **Certificates and Certificate Requests** table.
- Step 6** Moving your pointer to  icon in the **Details** column displays the certificate details information.

## Deleting a Certificate

To delete the certificate, click the delete icon. You can delete a certificate if it has expired or if you decide not to use third party certificates for VPN authentication.

## Certificate Revocation List (CRL)

A **Certificate Revocation List (CRL)** is a way to check the validity of an existing certificate. A certificate may be invalid for several reasons:

- The status of the entity identified by the Certificate has changed in some way (for example, an employee has left the company).
- The private key associated with a Certificate was stolen or compromised.
- A new certificate was issued that takes precedence over the old certificate.

If a certificate is invalid, the CA may publish the certificate on a **Certificate Revocation List** at a given interval, or on an online server in a X.509 v3 database using Online Certificate Status Protocol (OCSP). Consult your CA provider for specific details on locating a CRL file or URL.




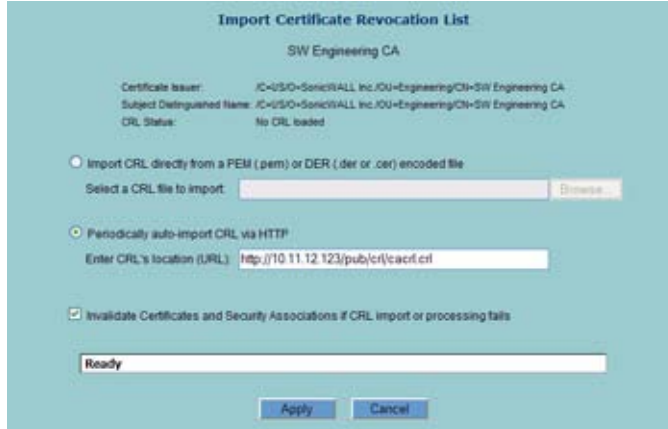
**Tip**

The SonicWALL security appliance supports obtaining the CRL via HTTP or manually downloading the list.

## Importing a CRL

You can import the CRL by manually downloading the CRL and then importing it into the SonicWALL security appliance.

- Step 1** Click on the Import certificate revocation list  icon. The Import CRL window is displayed.



- Step 2** You can import the CRL from the certificate file by selecting **Import CRL directly from a PEM (.pem) or DER (.der or .cer) encoded file**, and entering the path in the Select a CRL file to import field or click the **Browse** button to navigate to the file, click **Open**, then click **Import**.
- Step 3** You can also enter the URL location of the CRL by entering the address in the **Enter CRL's location (URL)** field, and then click **Import**. The CRL is downloaded automatically at intervals determined by the CA service. Certificates are checked against the CRL by the SonicWALL security appliance for validity when they are used.
- Step 4** By default, if no CRL is available, a Certificate is presumed to be valid if it passes all other checks (such as validity dates and signatures). To require that Certificates be checked against a valid CRL, enable the **Invalidate Certificates and Security Associations if CRL import or processing fails** setting.

## Generating a Certificate Signing Request



**Tip**

You should create a Certificate Policy to be used in conjunction with local certificates. A Certificate Policy determines the authentication requirements and the authority limits required for the validation of a certificate.

To generate a local certificate, follow these steps:

- Step 1** Click the **New Signing Request** button. The Certificate Signing Request window is displayed.

- Step 2** In the **Generate Certificate Signing Request** section, enter an alias name for the certificate in the **Certificate Alias** field.

- Step 3** Select the Request field type from the menu, then enter information for the certificate in the Request fields. As you enter information in the Request fields, the Distinguished Name (DN) is created in the **Subject Distinguished Name** field.

You can also attach an optional **Subject Alternative Name** to the certificate such as the **Domain Name** or **E-mail Address**.

- Step 4** The **Subject Key** type is preset as an **RSA** algorithm. RSA is a public key cryptographic algorithm used for encrypting data.

- Step 5** Select a Subject Key size from the **Subject Key Size** menu.



**Note** Not all key sizes are supported by a Certificate Authority, therefore you should check with your CA for supported key sizes.

- Step 6** Click **Generate** to create a certificate signing request file. Once the **Certificate Signing Request** is generated, a message describing the result is displayed.

- Step 7** Click **Export** to download the file to your computer, then click **Save** to save it to a directory on your computer. You have generated the **Certificate Request** that you can send to your Certificate Authority for validation.



# CHAPTER 9

## Configuring Time Settings

### System > Time

The **System > Time** page defines the time and date settings to time stamp log events, to automatically update SonicWALL Security Services, and for other internal purposes.

The screenshot shows the 'System > Time' configuration page. At the top right are 'Apply', 'Cancel', and a help icon. The 'System Time' section includes: 'Time (hh:mm:ss)' with input fields for 14, 05, and 22; 'Date' with dropdowns for December, 8, and 2004; and a 'Time Zone' dropdown menu set to 'Pacific Time (US & Canada) (GMT-8:00)'. Below these are four checkboxes: 'Set time automatically using NTP' (checked), 'Automatically adjust clock for daylight saving time' (checked), 'Display UTC in logs (instead of local time)' (unchecked), and 'Display date in international format' (unchecked). The 'NTP Settings' section has an 'Update Interval (minutes)' input field set to 30. At the bottom is an 'NTP Server' table with 'No Entries', an 'Add' button, and a 'Delete All' button. A 'Configure' link is also present. A note at the bottom states: 'Note: An internal NTP list is used by default, and the above list is optional.'

By default, the SonicWALL security appliance uses an internal list of public NTP servers to automatically update the time. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

### System Time

To select your time zone and automatically update the time, choose the time zone from the **Time Zone** menu. **Set time automatically using NTP** is activated by default to use NTP (Network Time Protocol) servers from an internal list to set time automatically. **Automatically adjust clock for daylight saving changes** is also activated by default to enable automatic adjustments for daylight savings time.

If you want to set your time manually, uncheck **Set time automatically using NTP**. Select the time in the 24-hour format using the **Time (hh:mm:ss)** menus and the date from the **Date** menus.

Selecting **Display UTC in logs (instead of local time)** specifies the use universal time (UTC) rather than local time for log events.

Selecting **Display time in International format** displays the date in International format, with the day preceding the month.

After selecting your System Time settings, click **Apply**.

## NTP Settings

Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes, to a fraction of a millisecond.



**Tip**

The SonicWALL security appliance uses an internal list of NTP servers so manually entering a NTP server is optional.

Select **Use NTP to set time automatically** if you want to use your local server to set the SonicWALL security appliance clock. You can also configure **Update Interval (minutes)** for the NTP server to update the SonicWALL security appliance. The default value is 60 minutes.

To add an NTP server to the SonicWALL security appliance configuration

**Step 1** Click **Add**. The **Add NTP Server** window is displayed.

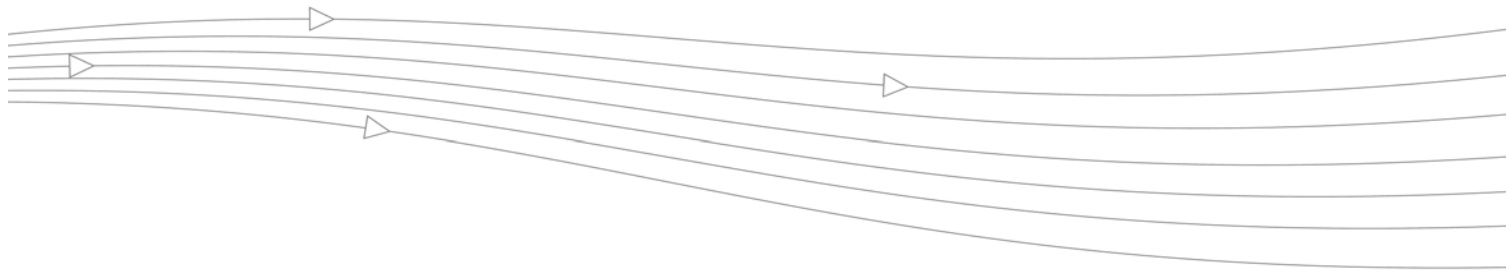


**Step 2** Type the IP address of an NTP server in the **NTP Server** field.

**Step 3** Click **OK**.

**Step 4** Click **Apply** on the **System > Time** page to update the SonicWALL security appliance.

To delete an NTP server, highlight the IP address and click **Delete**. Or, click **Delete All** to delete all servers.



# CHAPTER 10

## Setting Schedules

### System > Schedules

The **System > Schedules** page allows you to create and manage schedule objects for enforcing schedule times for a variety of SonicWALL security appliance features.



The **Schedules** table displays all your predefined and custom schedules. In the **Schedules** table, there are three default schedules: **Work Hours**, **After Hours**, and **Weekend Hours**. You can modify these schedules by clicking on the edit icon in the **Configure** column to display the **Edit Schedule** window.

**Note**

You cannot delete the default **Work Hours**, **After Hours**, or **Weekend Hours** schedules.

You apply schedule objects for the specific security feature. For example, if you add an access rule in the **Firewall > Access Rules** page, the **Add Rule** window provides a drop down menu of all the available schedule objects you created in the **System > Schedules** page.

A schedule can include multiple day and time increments for rule enforcement with a single schedule. If a schedule includes multiple day and time entries, a **+** (expand) button appears next to the schedule name. Clicking the **+** button expands the schedule to display all the day and time entries for the schedule.



## Adding a Schedule

To create schedules, click **Add**. The **Add Schedule** window is displayed.



- 
- Step 1** Enter a name for the schedule in the **Name** field.
  - Step 2** Select the days of the week to apply to the schedule or select **All**.
  - Step 3** Enter the time of day for the schedule to begin in the **Start** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
  - Step 4** Enter the time of day for the schedule to stop in the **Stop** field. The time must be in 24-hour format, for example, 17:00 for 5 p.m.
  - Step 5** Click **Add**.
  - Step 6** Click **OK** to add the schedule to the **Schedules** table.
  - Step 7** To delete existing days and times, select the schedule and click **Delete**. Or, to delete all existing schedules, click **Delete All**.

## Deleting Schedules

To delete individual schedule objects you created, select the checkbox next to the schedule entry, the **Delete** button becomes enabled. Click **Delete**. To delete all schedule objects you created, select the checkbox next to **Name** column header to select all schedules. Click **Delete**.



# CHAPTER 11

## Managing SonicWALL Security Appliance Firmware

### System > Settings

This **System > Settings** page allows you to manage your SonicWALL security appliance's SonicOS versions and preferences.

The screenshot displays the 'System > Settings' interface. At the top, there are 'Apply', 'Cancel', and a help icon. Below this is the 'Settings' section with 'Import Settings...' and 'Export Settings...' buttons. The 'Firmware Management' section includes a checked checkbox for 'Notify me when new firmware is available'. A table lists firmware images with columns for 'Firmware Image', 'Version', 'Date', 'Size', 'Download', and 'Boot'. At the bottom of the table are 'Upload New Firmware' and 'Create Backup' buttons. The 'FIPS' section at the very bottom has an unchecked checkbox for 'Enable FIPS Mode'.

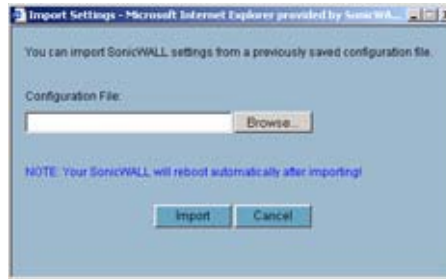
Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 3.2.0.0-14e	MON JAN 30 09:47:34 2006	4.76 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 3.2.0.0-14e	MON JAN 30 09:47:34 2006	4.76 MB		
Uploaded Firmware - New	SonicOS Enhanced 3.2.0.0-24e	MON JAN 30 09:47:32 2006	4.81 MB		
Uploaded Firmware with Factory Default Settings - New	SonicOS Enhanced 3.2.0.0-24e	MON JAN 30 09:47:32 2006	4.81 MB		
System Backup	SonicOS Enhanced 3.2.0.0-14e	MON JAN 30 09:25:44 2006	4.76 MB		

# Settings

## Import Settings

To import a previously saved preferences file into the SonicWALL security appliance, follow these instructions:

- Step 1** Click **Import Settings** to import a previously exported preferences file into the SonicWALL security appliance. The **Import Settings** window is displayed.



- Step 2** Click **Browse** to locate the file which has a \*.exp file name extension.  
**Step 3** Select the preferences file.  
**Step 4** Click **Import**, and restart the firewall.

## Export Settings

To export configuration settings from the SonicWALL security appliance, use the instructions below:

- Step 1** Click **Export Settings**. The **Export Settings** window is displayed.



- Step 2** Click **Export**.  
**Step 3** Click **Save**, and then select a location to save the file. The file is named "sonicwall.exp" but can be renamed.  
**Step 4** Click **Save**. This process can take up to a minute. The exported preferences file can be imported into the SonicWALL security appliance if it is necessary to reset the firmware.

## Firmware Management

The **Firmware Management** section provides settings that allow for easy firmware upgrade and preferences management. The **Firmware Management** section allows you to:

- Upload and download firmware images and system settings.

- Boot to your choice of firmware and system settings.
- Manage system backups.
- Easily return your SonicWALL security appliance to the previous system state.

**Note**

SonicWALL security appliance **SafeMode**, which uses the same settings used **Firmware Management**, provides quick recovery from uncertain configuration states.

## Automatic Notification of New Firmware

To receive automatic notification of new firmware, select the **Notify me when new firmware is available** check box. If you enable this feature, the SonicWALL security appliance sends a status message to the SonicWALL firmware server daily with the following information:

- **SonicWALL Serial Number**
- **Product Type**
- **Current Firmware Version**
- **Language**
- **Currently Available Memory**
- **ROM Version**

**Caution** After the initial 90 days from purchase, firmware updates are available only to registered users with a valid support contract. You must register your SonicWALL at <https://www.mysonicwall.com>.

If a new firmware version becomes available, the message **New SonicWALL Firmware Version is available**. Click here for details on this latest release appears in System Messages on the **System > Status** page. Clicking the here link displays the Release Notes for the new firmware.

## Firmware Management Table

Firmware Image	Version	Date	Size	Download	Boot
Current Firmware	SonicOS Enhanced 3.2.0.0-14a	MON JAN 30 09:47:34 2006	4.76 MB		
Current Firmware with Factory Default Settings	SonicOS Enhanced 3.2.0.0-14a	MON JAN 30 09:47:34 2006	4.76 MB		
Uploaded Firmware - New!	SonicOS Enhanced 3.2.0.0-24a	MON JAN 30 09:47:32 2006	4.81 MB		
Uploaded Firmware with Factory Default Settings - New!	SonicOS Enhanced 3.2.0.0-24a	MON JAN 30 09:47:32 2006	4.81 MB		
System Backup	SonicOS Enhanced 3.2.0.0-14a	MON JAN 30 09:25:44 2006	4.76 MB		

The Firmware Management table displays the following information:

- **Firmware Image** - in this column, four types of firmware images are listed:
  - **Current Firmware** - firmware currently loaded on the SonicWALL security appliance.
  - **Current Firmware with Factory Default Settings** - rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, username, and password.
  - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**.

- **Uploaded Firmware** - the latest uploaded version from mySonicWALL.com.
  - **Uploaded Firmware with Factory Default Settings** - the latest version uploaded with factory default settings.
  - **Uploaded Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**.
- **Version** - the firmware version.
  - **Date** - the day, date, and time of downloading the firmware.
  - **Size** - the size of the firmware file in Megabytes (MB).
  - **Download** - clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
  - **Boot** - clicking the icon reboots the SonicWALL security appliance with the firmware version listed in the same row.

---

**Caution** Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the **Current Firmware** image.

---



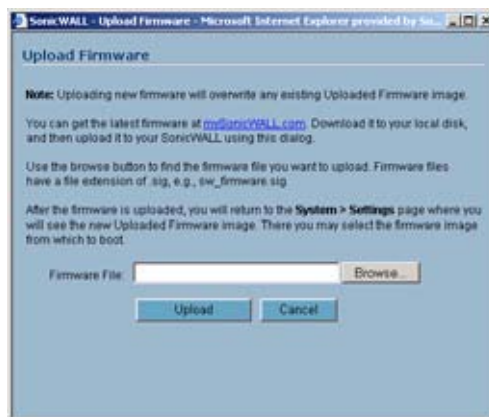
---

**Caution** When uploading firmware to the SonicWALL security appliance, you must not interrupt the Web browser by closing the browser, clicking a link, or loading a new page. If the browser is interrupted, the firmware may become corrupted.

---

## Updating Firmware Manually

Click **Upload New Firmware** to upload new firmware to the SonicWALL security appliance. The **Upload Firmware** window is displayed. Browse to the firmware file located on your local drive. Click **Upload** to upload the new firmware to the SonicWALL security appliance.



## Creating a Backup Firmware Image

When you click **Create Backup**, the SonicWALL security appliance takes a “snapshot” of your current system state, firmware and configuration preferences, and makes it the new System Backup firmware image. Clicking **Create Backup** overwrites the existing **System Backup** firmware image as necessary.

## SafeMode - Rebooting the SonicWALL Security Appliance

SafeMode allows easy firmware and preferences management as well as quick recovery from uncertain configuration states. It is no longer necessary to reset the firmware by pressing and holding the Reset button on the appliance. Pressing the Reset button for one second launches the SonicWALL security appliance into SafeMode. SafeMode allows you to select the firmware version to load and reboot the SonicWALL security appliance.

To access the SonicWALL security appliance using SafeMode, press the Reset button for 1 second. After the SonicWALL security appliance reboots, open your Web browser and enter the current IP address of the SonicWALL security appliance or the default IP address: *192.168.168.168*. The SafeMode page is displayed:

SafeMode allows you to do any of the following:

- Upload and download firmware images to the SonicWALL security appliance.
- Upload and download system settings to the SonicWALL security appliance.
- Boot to your choice of firmware options.
- Create a system backup file.
- Return your SonicWALL security appliance to a previous system state.

## System Information

System Information for the SonicWALL security appliance is retained and displayed in this section.

## Firmware Management

The **Firmware Management** table in SafeMode has the following columns:

- **Firmware Image** - In this column, five types of firmware images are listed:
  - **Current Firmware**, firmware currently loaded on the SonicWALL security appliance
  - **Current Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
  - **Current Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
  - **Uploaded Firmware**, the last version uploaded from mysonicwall.com
  - **Uploaded Firmware with Factory Default Settings**, rebooting using this firmware image resets the SonicWALL security appliance to its default IP addresses, user name, and password
  - **Uploaded Firmware with Backup Settings** - a firmware image created by clicking **Create Backup**
- **Version** - The firmware version is listed in this column.
- **Date** - The day, date, and time of downloading the firmware.
- **Size** - The size of the firmware file in Megabytes (MB).
- **Download** - Clicking the icon saves the firmware file to a new location on your computer or network. Only uploaded firmware can be saved to a different location.
- **Boot** - Clicking the icon reboots the SonicWALL security appliance with the firmware version listed in the same row.

**Note**

---

Clicking **Boot** next to any firmware image overwrites the existing current firmware image making it the Current Firmware image.

---

Click **Boot** in the firmware row of your choice to restart the SonicWALL security appliance.

## FIPS

When operating in FIPS (Federal Information Processing Standard) Mode, the SonicWALL security appliance supports FIPS 140-2 Compliant security. Among the FIPS-compliant features of the SonicWALL security appliance include PRNG based on SHA-1 and only FIPS-approved algorithms are supported (DES, 3DES, and AES with SHA-1).

Select **Enable FIPS Mode** to enable the SonicWALL security appliance to comply with FIPS. When you check this setting, a dialog box is displayed with the following message: **Warning! Modifying the FIPS mode will disconnect all users and restart the device. Click OK to proceed.**

Click **OK** to reboot the security appliance in FIPS mode. A second warning displays. Click **Yes** to continue rebooting. To return to normal operation, uncheck the **Enable FIPS Mode** check box and reboot the SonicWALL security appliance into non-FIPS mode.

**Caution**

---

When using the SonicWALL security appliance for FIPS-compliant operation, the tamper-evident sticker that is affixed to the SonicWALL security appliance must remain in place and untouched.

---





## CHAPTER 12

# Using SonicWALL Packet Capture

---

## System > Packet Capture

This chapter contains the following sections:

- [“Packet Capture Overview” on page 105](#)
- [“Using Packet Capture” on page 107](#)
- [“Verifying Packet Capture Activity” on page 120](#)
- [“Related Information” on page 122](#)

## Packet Capture Overview

This section provides an introduction to the SonicWALL SonicOS Enhanced packet capture feature. This section contains the following subsections:

- [“What is Packet Capture?” on page 105](#)
- [“Benefits” on page 106](#)
- [“How Does Packet Capture Work?” on page 106](#)

## What is Packet Capture?

Packet capture is a mechanism that allows you to capture and examine the contents of individual data packets that traverse your SonicWALL firewall appliance. The captured packets contain both data and addressing information. The captured addressing information from the packet header includes the following:

- Interface identification
- MAC addresses
- Ethernet type
- Internet Protocol (IP) type
- Source and destination IP addresses
- Port numbers
- L2TP payload details

- PPP negotiations details

You can configure the packet capture feature in the SonicOS Enhanced user interface (UI). The UI provides a way to configure the capture criteria, display settings, and file export settings, and displays the captured packets.

## Benefits

The SonicOS Enhanced packet capture feature provides the functionality and flexibility that you need to examine network traffic without the use of external utilities, such as Wireshark (formerly known as Ethereal). SonicOS Enhanced 4.0 and above include the following improvements in the packet capture tool:

- Capture control mechanism with improved granularity for custom filtering
- Display filter settings independent from capture filter settings
- Packet status indicates if the packet was dropped, forwarded, generated, or consumed by the firewall
- Three-window output in the UI:
  - List of packets
  - Decoded output of selected packet
  - Hexadecimal dump of selected packet
- Export capabilities include text or HTML format with hex dump of packets, plus CAP file format
- Automatic export to FTP server when the buffer is full
- Bidirectional packet capture based on IP address and port
- Configurable wrap-around of packet capture buffer when full

## How Does Packet Capture Work?

As an administrator, you can configure the general settings, capture filter, display filter, advanced settings, and FTP settings of the packet capture tool. As network packets enter the packet capture subsystem, the capture filter settings are applied and the resulting packets are written to the capture buffer. The display filter settings are applied as you view the buffer contents in the UI. You can log the capture buffer to view in the UI, or you can configure automatic transfer to the FTP server when the buffer is full.

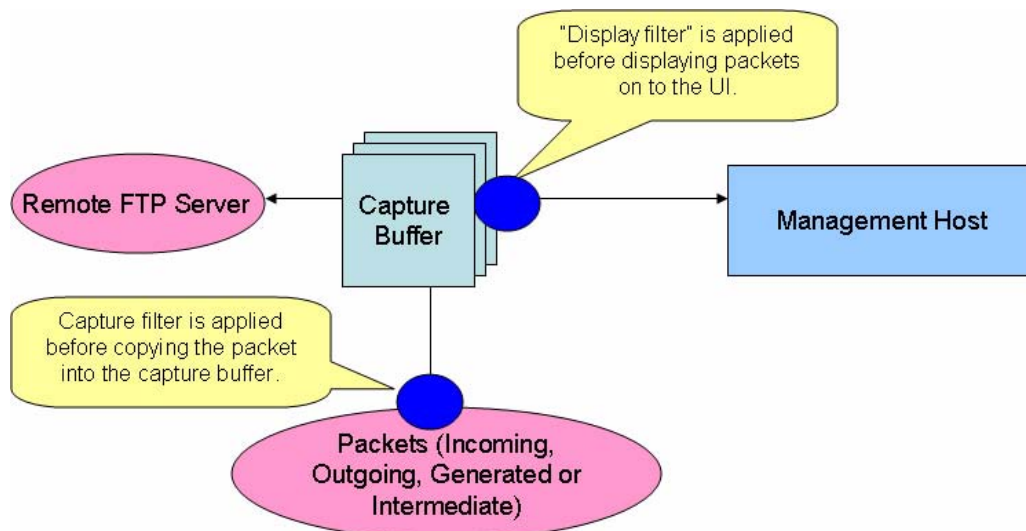
Default settings are provided so that you can start using packet capture without configuring it first. The basic functionality is as follows:

- |               |  |
|---------------|--|
| <b>Start:</b> | Click <b>Start</b> to begin capturing all packets except those used for communication between the SonicWALL appliance and the UI on your console system. |
| <b>Stop:</b>  | Click <b>Stop</b> to stop the packet capture.  |
| <b>Reset:</b> | Click <b>Reset</b> to clear the status counters that are displayed at the top of the Packet Capture page.  |

- Refresh:** Click Refresh to display new buffer data in the Captured Packets window. You can then click any packet in the window to display its header information and data in the Packet Detail and Hex Dump windows.
- Export As:** Display or save a snapshot of the current buffer in the file format that you select from the drop-down list. Saved files are placed on your local management system (where the UI is running). Choose from the following formats:
- **CAP** - Select CAP format if you want to view the data with the Wireshark (formerly Ethereal) network protocol analyzer. This is also known as libcap or pcap format. A dialog box allows you to open the buffer file with Wireshark, or save it to your local hard drive with the extension **.pcap**.
  - **HTML** - Select HTML to view the data with a browser. You can use File > Save As to save a copy of the buffer to your hard drive.
  - **Text** - Select Text to view the data in a text editor. A dialog box allows you to open the buffer file with the registered text editor, or save it to your local hard drive with the extension **.wri**.

Refer to the figure below to see a high level view of the packet capture subsystem. This shows the different filters and how they are applied.

**Figure 12:1 High level packet capture on subsystem view**



## Using Packet Capture

This section contains the following subsections:

- [“Accessing Packet Capture in the UI” on page 108](#)
- [“Starting and stopping packet capture” on page 108](#)
- [“Viewing the captured packets” on page 109](#)

## Accessing Packet Capture in the UI

This section describes how to access the packet capture tool in the SonicOS UI. There are two ways to access the Packet Capture screen.

- Step 1** Log in to the SonicOS UI as admin.
- Step 2** To go directly to the Packet Capture screen, in the left pane, under **System**, click **Packet Capture**.

- Step 3** Alternatively, to access packet capture from the Diagnostics screen, in the left pane, under **System**, click **Diagnostics**.
- Step 4** In the right pane, in the Diagnostic Tool list, click **Packet Capture**.

## Starting and stopping packet capture

The Packet Capture screen has buttons for starting and stopping a packet capture. You can start a packet capture that uses default settings without configuring specific criteria for packet capture, display, FTP export, and other settings. If you start a default packet capture, the SonicWALL appliance will capture all packets except those for internal communication, and will stop when the buffer is full or when you click Stop.

## Starting packet capture

- 
- Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.
- Step 2** Under **Packet Capture**, optionally click **Reset**. The Packet Capture page displays several lines of statistics above the Start and Stop buttons. You can click Reset to set the statistics back to zero.
- Step 3** Under **Packet Capture**, click **Start**.
- Step 4** To refresh the packet display windows to show new buffer data, click **Refresh**.  
You can view the captured packets in the Captured Packets, Packet Detail, and Hex Dump sections of the screen. See “Viewing the captured packets” on page 109.

## Stopping packet capture

- 
- Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.
- Step 2** Under **Packet Capture**, click **Stop**.

## Viewing the captured packets

The UI provides three windows to display different views of the captured packets. The following sections describe the viewing windows:

- [“About the Captured Packets Window” on page 109](#)
- [“About the Packet Detail Window” on page 111](#)
- [“About the Hex Dump Window” on page 111](#)

## About the Captured Packets Window

The **Captured Packets** window displays the following statistics about each packet:

- # - The packet number relative to the start of the capture
- Time - The date and time that the packet was captured
- Ingress - The SonicWALL appliance interface on which the packet arrived is marked with an asterisk (\*). The subsystem type abbreviation is shown in parentheses. Subsystem type abbreviations are defined in the following table.

Abbreviation	Definition
i	Interface
hc	Hardware based encryption or decryption
sc	Software based encryption or decryption
m	Multicast
r	Packet reassembly
s	System stack
ip	IP helper
f	Fragmentation

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	08/24/2006 10:43:59.928	X1'(i)	--	10.0.202.243	10.50.128.53	ARP	Request	--	Consumed, Module Id:45	60[60]
2	08/24/2006 10:44:00.000	X1*(i)	--	0.0.0.0	10.0.81.101	ARP	Request	--	Consumed, Module Id:45	60[60]
3	08/24/2006 10:44:00.016	X1*(i)	--	10.0.202.243	10.50.128.53	ARP	Request	--	Consumed, Module Id:45	60[60]
4	08/24/2006 10:44:00.048	X0*(hc)	X1	10.0.93.43	10.0.93.21	IP	ESP	--	Consumed, Module Id:45	302[302]

- Egress - The SonicWALL appliance interface on which the packet was captured when sent out
  - The subsystem type abbreviation is shown in parentheses. See the table above for definitions of subsystem type abbreviations
- Source IP - The source IP address of the packet
- Destination IP - The destination IP address of the packet
- Ether Type - The Ethernet type of the packet from its Ethernet header
- Packet Type - The type of the packet depending on the Ethernet type; for example:
  - For IP packets, the packet type might be TCP, UDP, or another protocol that runs over IP
  - For PPPoE packets, the packet type might be PPPoE Discovery or PPPoE Session
  - For ARP packets, the packet type might be Request or Reply
- Ports [Src,Dst] - The source and destination TCP or UDP ports of the packet
- Status - The status field for the packet

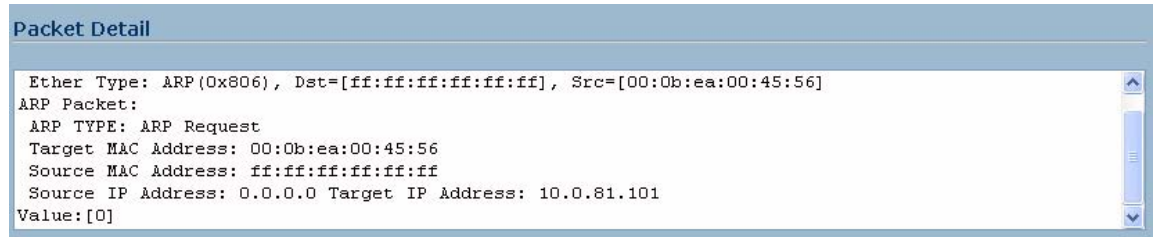
The status field shows the state of the packet with respect to the firewall. A packet can be dropped, generated, consumed or forwarded by the SonicWALL appliance. You can position the mouse pointer over dropped or consumed packets to show the following information.

Packet status	Displayed value	Definition of displayed value
Dropped	Module-ID = <integer>	Value for the protocol subsystem ID
	Drop-code = <integer>	Reason for dropping the packet
	Reference-ID: <code>	SonicWALL-specific data
Consumed	Module-ID = <integer>	Value for the protocol subsystem ID

- Length [Actual] - Length value is the number of bytes captured in the buffer for this packet. Actual value, in brackets, is the number of bytes transmitted in the packet.  
You can configure the number of bytes to capture. See “Configuring General Settings” on page 112.

## About the Packet Detail Window

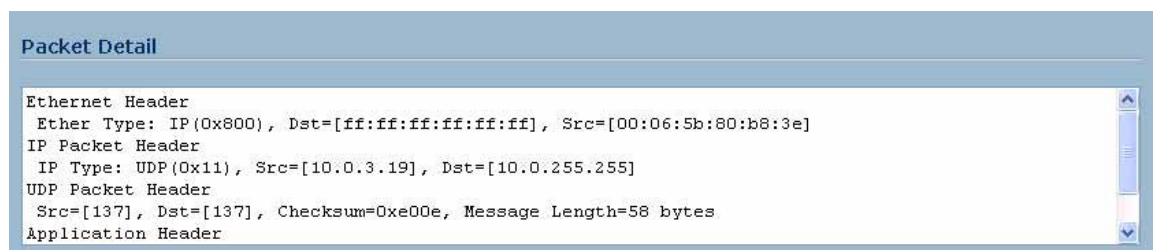
When you click on a packet in the Captured Packets window, the packet header fields are displayed in the Packet Detail window. The display will vary depending on the type of packet that you select.



```

Packet Detail
-----
Ether Type: ARP(0x806), Dst=[ff:ff:ff:ff:ff:ff], Src=[00:0b:ea:00:45:56]
ARP Packet:
  ARP TYPE: ARP Request
  Target MAC Address: 00:0b:ea:00:45:56
  Source MAC Address: ff:ff:ff:ff:ff:ff
  Source IP Address: 0.0.0.0 Target IP Address: 10.0.81.101
Value:[0]

```



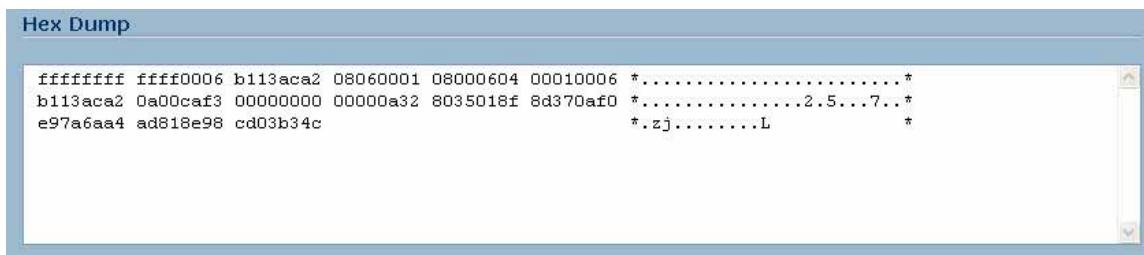
```

Packet Detail
-----
Ethernet Header
  Ether Type: IP(0x800), Dst=[ff:ff:ff:ff:ff:ff], Src=[00:06:5b:80:b8:3e]
IP Packet Header
  IP Type: UDP(0x11), Src=[10.0.3.19], Dst=[10.0.255.255]
UDP Packet Header
  Src=[137], Dst=[137], Checksum=0xe00e, Message Length=58 bytes
Application Header

```

## About the Hex Dump Window

When you click on a packet in the Captured Packets window, the packet data is displayed in hexadecimal and ASCII format in the Hex Dump window. The hex format is shown on the left side of the window, with the corresponding ASCII characters displayed to the right for each line. When the hex value is zero, the ASCII value is displayed as a dot.



```

Hex Dump
-----
ffffff ffff0006 b113aca2 08060001 08000604 00010006 *.....*
b113aca2 0a00caf3 00000000 00000a32 8035018f 8d370af0 *.....2.5..7.*
e97a6aa4 ad818e98 cd03b34c *..zj.....L*

```

## Configuring Packet Capture

You can access the packet capture tool on the System > Packet Capture page of the SonicOS UI. There are five main areas of configuration for the packet capture tool. The following sections describe the configuration options, and provide procedures for accessing and configuring packet capture:

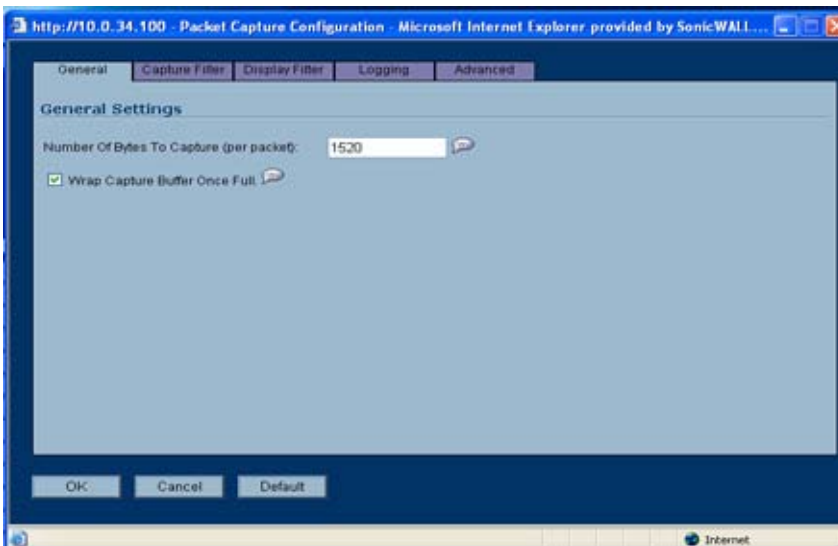
- [“Configuring General Settings” on page 112](#)
- [“Configuring Capture Filter Settings” on page 112](#)
- [“Configuring Display Filter Settings” on page 115](#)
- [“Configuring Logging Settings” on page 117](#)

- [“Configuring Advanced Settings” on page 119](#)
- [“Restarting FTP logging” on page 120](#)

## Configuring General Settings

This section describes how to configure packet capture general settings, including the number of bytes to capture per packet and the buffer wrap option. You can specify the number of bytes using either decimal or hexadecimal, with a minimum value of 14. The buffer wrap option enables the packet capture to continue even when the buffer becomes full, by overwriting the buffer from the beginning.

- 
- Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.
- Step 2** Under **Packet Capture**, click **Configure**.
- Step 3** In the **Packet Capture Configuration** window, click the **General** tab.



- Step 4** In the **Number of Bytes To Capture (per packet)** box, type a number. The minimum value is 14.
- Step 5** To continue capturing packets after the buffer fills up, select the **Wrap Capture Buffer Once Full** checkbox. Selecting this option will cause packet capture to start writing captured packets at the beginning of the buffer again after the buffer fills.
- Step 6** Click **OK**.

## Configuring Capture Filter Settings

This section describes how to configure packet capture filter settings, including the following:

- Interface on your SonicWALL appliance  
You can specify up to ten interfaces separated by commas. Refer to the Network > Interfaces screen in the UI for the available interface names. You can use a negative value to configure all interfaces except the one(s) specified; for example: !X0, or !LAN. For the TZ 190, you could specify WAN, LAN, WWAN, OPT, or !WWAN, !OPT.
- Ethernet type of the packets that you want to capture



You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported: ARP, IP, PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone. This option is not case-sensitive. For example, to capture all supported types, you could enter: ARP, IP, PPPOE. You can use one or more negative values to capture all Ethernet types except those specified; for example: !ARP, !PPPoE. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS Enhanced. See “Supported Packet Types” on page 122.

- IP type of the packets that you want to capture

You can specify up to ten IP types separated by commas. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP. This option is not case-sensitive. You can use one or more negative values to capture all IP types except those specified; for example: !TCP, !UDP. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See “Supported Packet Types” on page 122.

- Source IP addresses from which to capture packets

You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets from all but the specified addresses; for example: !10.3.3.3, !10.4.4.4.

- Source port(s) from which to capture packets

You can specify up to ten port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets from all but the specified ports; for example: !80, !8080.

- Destination IP address(es) for which to capture packets

You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to capture packets destined for all but the specified addresses; for example: !10.3.3.3, !10.4.4.4.

- Destination port(s) for which to capture packets

You can specify up to ten port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets destined for all but the specified ports; for example: !80, !8080.

- Bidirectional address and port mapping

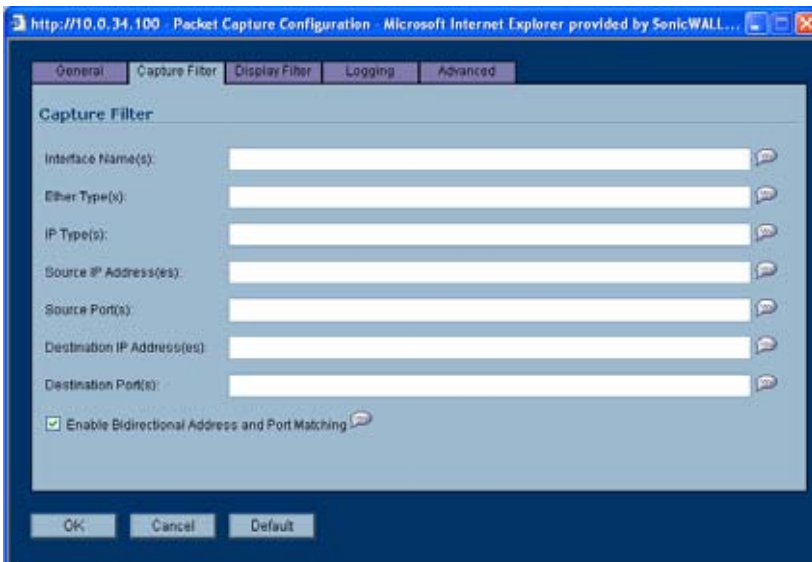
When this option is selected, IP addresses and ports specified here will be matched against both the source and destination fields in each packet.


**Note**

If a field is left blank, no filtering is done on that field. Packets are captured without regard to the value contained in that field of their headers.

To configure Packet Capture complete the following steps:

- Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.
- Step 2** Under **Packet Capture**, click **Configure**.
- Step 3** In the **Packet Capture Configuration** window, click the **Capture Filter** tab.



- Step 4** In the **Interface Name(s)** box, type the SonicWALL appliance interfaces on which to capture packets, or use the negative format (!X0) to capture packets from all interfaces except those specified. To capture on all interfaces, leave blank.
- Step 5** In the **Ether Type(s)** box, enter the Ethernet types for which you want to capture packets, or use the negative format (!ARP) to capture packets from all Ethernet types except those specified. To capture all Ethernet types, leave blank.
- Step 6** In the **IP Type(s)** box, enter the IP packet types for which you want to capture packets, or use the negative format (!UDP) to capture packets from all IP types except those specified. To capture all IP types, leave blank.
- Step 7** In the **Source IP Address(es)** box, type the IP addresses from which you want to capture packets, or use the negative format (!10.1.2.3) to capture packets from all source addresses except those specified. To capture packets from all source addresses, leave blank.
- Step 8** In the **Source Port(s)** box, type the port numbers from which you want to capture packets, or use the negative format (!25) to capture packets from all source ports except those specified. To capture packets from all source ports, leave blank.
- Step 9** In the **Destination IP Address(es)** box, type the IP addresses for which you want to capture packets, or use the negative format (!10.1.2.3) to capture packets with all destination addresses except those specified. To capture packets for all destination addresses, leave blank.
- Step 10** In the **Destination Port(s)** box, type the port numbers for which you want to capture packets, or use the negative format (!80) to capture packets with all destination ports except those specified. To capture packets for all destination ports, leave blank.
- Step 11** To match the values in the source and destination fields against either the source or destination information in each packet, select the **Enable Bidirectional Address and Port Matching** checkbox.

## Configuring Display Filter Settings

This section describes how to configure packet capture display filter settings. The values that you provide here are compared to corresponding fields in the captured packets, and only those packets that match are displayed. Display filter settings include the following:

- Interface on your SonicWALL appliance  
 You can specify up to ten interfaces separated by commas. Refer to the Network > Interfaces screen in the UI for the available interface names. You can use a negative value to configure all interfaces except the one(s) specified; for example: !X0, or !LAN. For the TZ 190, you could specify WAN, LAN, WWAN, OPT, or !WWAN, !OPT.
- Ethernet type of the packets that you want to display  
 You can specify up to ten Ethernet types separated by commas. Currently, the following Ethernet types are supported: ARP, IP, PPPoE-SES, and PPPoE-DIS. The latter two can be specified by PPPoE alone. This option is not case-sensitive. For example, to display all supported types, you could enter: ARP, IP, PPPOE. You can use one or more negative values to display all Ethernet types except those specified; for example: !ARP, !PPPoE. You can also use hexadecimal values to represent the Ethernet types, or mix hex values with the standard representations; for example: ARP, 0x800, IP. Normally you would only use hex values for Ethernet types that are not supported by acronym in SonicOS Enhanced. See “Supported Packet Types” on page 122.
- IP type of the packets that you want to display  
 You can specify up to ten IP types separated by commas. The following IP types are supported: TCP, UDP, ICMP, GRE, IGMP, AH, ESP. This option is not case-sensitive. You can use one or more negative values to display all IP types except those specified; for example: !TCP, !UDP. You can also use hexadecimal values to represent the IP types, or mix hex values with the standard representations; for example: TCP, 0x1, 0x6. See “Supported Packet Types” on page 122.
- Source IP addresses from which to display packets  
 You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to display packets with all but the specified source addresses; for example: !10.3.3.3, !10.4.4.4.
- Source port(s) from which to display packets  
 You can specify up to ten port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to display packets with all but the specified source ports; for example: !80, !8080.
- Destination IP address(es) for which to display packets  
 You can specify up to ten IP addresses separated by commas; for example: 10.1.1.1, 192.2.2.2. You can use one or more negative values to display packets with all but the specified destination addresses; for example: !10.3.3.3, !10.4.4.4.
- Destination port(s) for which to display packets  
 You can specify up to ten port numbers separated by commas; for example: 20, 21, 22, 25. You can use one or more negative values to capture packets with all but the specified destination ports; for example: !80, !8080.
- Bidirectional address and port mapping  
 When this option is selected, IP addresses and ports specified in either the source or destination fields are matched against both the source and destination fields in each packet.
- Packet status values

SonicOS Enhanced adds one of four possible packet status values to each captured packet: forwarded, generated, consumed, and dropped. You can select one or more of these status values to match when displaying packets. The status value shows the state of the packet with respect to the firewall, as follows:

- Forwarded - The packet arrived on one interface and the SonicWALL appliance sent it out on another interface.
- Generated - The SonicWALL appliance created the packet during the process of encryption or decryption, fragmentation or reassembly, or as a result of certain protocols.
- Consumed - The packet was destined for the SonicWALL appliance.
- Dropped - The SonicWALL appliance did nothing further with the packet. The firewall might have identified the packet as malformed, malicious, on the deny list, or not on the allow list.

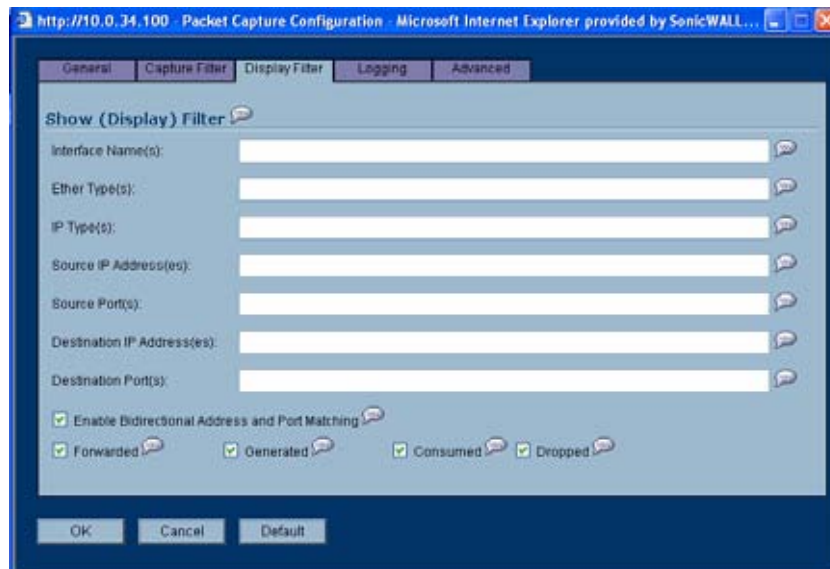
**Note**

If a field is left blank, no filtering is done on that field. Packets are displayed without regard to the value contained in that field of their headers.

**Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.

**Step 2** Under **Packet Capture**, click **Configure**.

**Step 3** In the **Packet Capture Configuration** window, click the **Display Filter** tab.



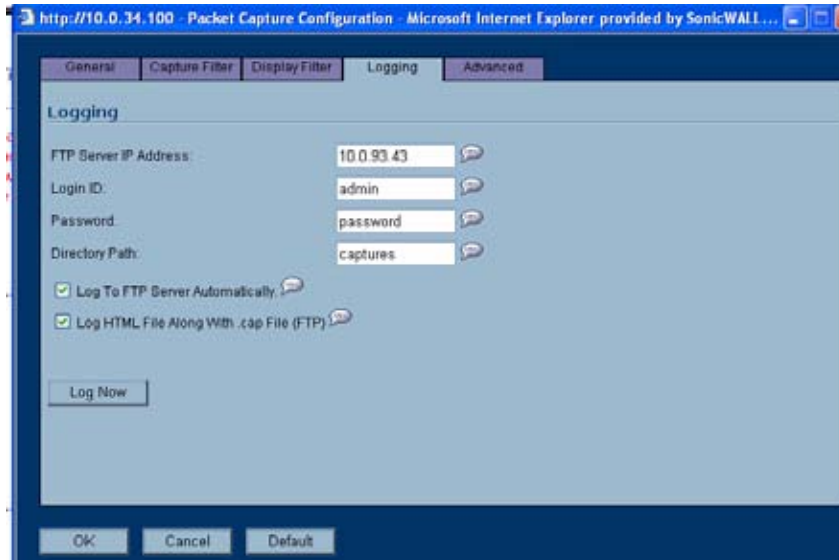
- Step 4** In the **Interface Name(s)** box, type the SonicWALL appliance interfaces for which to display packets, or use the negative format (!X0) to display packets captured from all interfaces except those specified. To display packets captured on all interfaces, leave blank.
- Step 5** In the **Ether Type(s)** box, enter the Ethernet types for which you want to display packets, or use the negative format (!ARP) to display packets of all Ethernet types except those specified. To display all Ethernet types, leave blank.
- Step 6** In the **IP Type(s)** box, enter the IP packet types for which you want to display packets, or use the negative format (!UDP) to display packets of all IP types except those specified. To display all IP types, leave blank.
- Step 7** In the **Source IP Address(es)** box, type the IP addresses from which you want to display packets, or use the negative format (!10.1.2.3) to display packets captured from all source addresses except those specified. To display packets from all source addresses, leave blank.
- Step 8** In the **Source Port(s)** box, type the port numbers from which you want to display packets, or use the negative format (!25) to display packets captured from all source ports except those specified. To display packets from all source ports, leave blank.
- Step 9** In the **Destination IP Address(es)** box, type the IP addresses for which you want to display packets, or use the negative format (!10.1.2.3) to display packets with all destination addresses except those specified. To display packets for all destination addresses, leave blank.
- Step 10** In the **Destination Port(s)** box, type the port numbers for which you want to display packets, or use the negative format (!80) to display packets with all destination ports except those specified. To display packets for all destination ports, leave blank.
- Step 11** To match the values in the source and destination fields against either the source or destination information in each captured packet, select the **Enable Bidirectional Address and Port Matching** checkbox.
- Step 12** To display captured packets that the SonicWALL appliance forwarded, select the **Forwarded** checkbox.
- Step 13** To display captured packets that the SonicWALL appliance generated, select the **Generated** checkbox.
- Step 14** To display captured packets that the SonicWALL appliance consumed, select the **Consumed** checkbox.
- Step 15** To display captured packets that the SonicWALL appliance dropped, select the **Dropped** checkbox.

## Configuring Logging Settings

This section describes how to configure packet capture logging settings. These settings provide a way to configure automatic logging of the capture buffer to an external FTP server. When the buffer fills up, the packets are transferred to the FTP server. The capture continues without interruption.

If you configure automatic logging, this supersedes the setting for wrapping the buffer when full. With automatic FTP logging, the capture buffer is effectively wrapped when full, but you also retain all the data rather than overwriting it each time the buffer wraps.

- Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.



- Step 2** Under **Packet Capture**, click **Configure**.
- Step 3** In the **Packet Capture Configuration** window, click the **Logging** tab.
- Step 4** In the **FTP Server IP Address** box, type the IP address of the FTP server. For example, type 10.1.2.3.



**Note** Make sure that the FTP server IP address is reachable by the SonicWALL appliance. An IP address that is reachable only via a VPN tunnel is not supported.

- Step 5** In the **Login ID** box, type the login name that the SonicWALL appliance should use to connect to the FTP server.
- Step 6** In the **Password** box, type the password that the SonicWALL appliance should use to connect to the FTP server.
- Step 7** In the **Directory Path** box, type the directory location for the transferred files. The files are written to this location relative to the default FTP root directory. For libcap format, files are named “packet-log--<>.cap”, where the <> contains a run number and date including hour,

month, day, and year. For example, packet-log--3-22-08292006.cap. For HTML format, file names are in the form: "packet-log\_h-<>.html". An example of an HTML file name is: packet-log\_h-3-22-08292006.html.

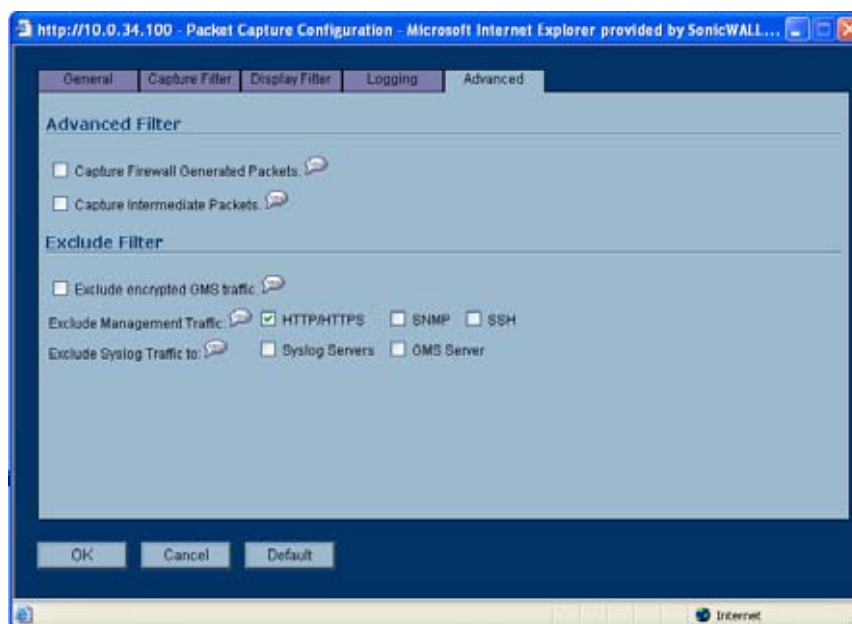
- Step 8** To enable automatic transfer of the capture file to the FTP server when the buffer is full, select the **Log To FTP Server Automatically** checkbox. Files are transferred in both libcap and HTML format.
- Step 9** To enable transfer of the file in HTML format as well as libcap format, select the **Log HTML File Along With .cap File (FTP)**.
- Step 10** To test the connection to the FTP server and transfer the capture buffer contents to it, click **Log Now**. In this case the file name will contain an 'F'. For example, packet-log-F-3-22-08292006.cap or packet-log\_h-F-3-22-08292006.html.
- Step 11** To save your settings and exit the screen, click **OK**.

## Configuring Advanced Settings

This section describes how to configure settings for the following:

- Capturing packets generated by the SonicWALL appliance
- Capturing intermediate packets generated by the appliance
- Excluding traffic from SonicWALL Global Management System (GMS)
- Excluding management traffic
- Excluding syslog traffic

- Step 1** Navigate to the **Packet Capture** page in the UI. See "Accessing Packet Capture in the UI" on page 108.
- Step 2** Under **Packet Capture**, click **Configure**.
- Step 3** In the **Packet Capture Configuration** window, click the **Advanced** tab.



- Step 4** To capture packets generated by the SonicWALL appliance, select the **Capture Firewall Generated Packets** checkbox.

Even when interfaces specified in the capture filters do not match, this option ensures that packets generated by the SonicWALL appliance are captured. This includes packets generated by HTTP(S), L2TP, DHCP servers, PPP, PPPOE, and routing protocols. Captured packets are marked with 's' in the incoming interface area when they are from the system stack. Otherwise, the incoming interface is not specified.

- Step 5** To capture intermediate packets generated by the SonicWALL appliance, select the **Capture Intermediate Packets** checkbox.
- Intermediate packets include packets generated as a result of fragmentation or reassembly, intermediate encrypted packets, IP helper generated packets, and replicated multicast packets.
- Step 6** To exclude encrypted management or syslog traffic to or from GMS, select the **Exclude encrypted GMS traffic** checkbox.
- This setting only affects encrypted traffic within a configured primary or secondary GMS tunnel. GMS management traffic is not excluded if it is sent via a separate tunnel.
- Step 7** To exclude management traffic, select the **Exclude Management Traffic** checkbox and select one or more checkboxes for **HTTP/HTTPS**, **SNMP**, or **SSH**. If management traffic is sent via a tunnel, the packets are not excluded.
- Step 8** To exclude syslog traffic to a server, select the **Exclude Syslog Traffic** checkbox and select one or more checkboxes for **Syslog Servers** or **GMS Server**. If syslog traffic is sent via a tunnel, the packets are not excluded.

## Restarting FTP logging

If automatic FTP logging is off, either because of a failed connection or simply disabled, you can restart it in **Configure > Logging**.

- Step 1** Navigate to the **Packet Capture** page in the UI. See “Accessing Packet Capture in the UI” on page 108.
- Step 2** Under **Packet Capture**, click **Configure**.
- Step 3** In the **Packet Capture Configuration** window, click the **Logging** tab.
- Step 4** Verify that the settings are correct for each item on the page. See “Configuring Logging Settings” on page 117.
- Step 5** To change the FTP logging status on the main packet capture page to “active”, select the **Log To FTP Server Automatically** checkbox.
- Step 6** Click **OK**.

## Verifying Packet Capture Activity

This section describes how to tell if your packet capture is working correctly according to the configuration. It contains the following sections:

- [“Understanding Status Indicators” on page 120](#)
- [“Resetting the Status Information” on page 122](#)

## Understanding Status Indicators

The main Packet Capture screen displays status indicators for packet capture and FTP logging. The packet capture status indicator shows one of the following three conditions:



- Red: Capture is stopped
- Green: Capture is running and the buffer is not full
- Orange: Capture is running, but the buffer is full

**System > Packet Capture**

Packet Capture

Trace active, Buffer size 2000 KB, 12120 Packets captured, Buffer is 99% Full, 0 MB of Buffer lost

FTP logging off, FTP Server Pass/Failure count: 0 / 0, FTP Thread is Idle, Buffer is FULL

Current Buffer Statistics: 769 Dropped, 9080 Forwarded, 1141 Consumed, 1139 Generated, 0 Unknowns

Current Configurations: Filters | General | Logging

Buttons: Configure | Start | Stop | Reset | Refresh | Export as: [dropdown]

Items: 1 to 50 of 12120

#	Time	Ingress	Egress	Source IP	Destination IP	Ether Type	Packet Type	Ports[Src, Dst]	Status	Length [Actual]
1	02/14/2007 13:33:39.864	X0*(0)	-	192.168.168.100	192.168.168.255	IP	UDP	137,137	DROPPED	92[92]
2	02/14/2007 13:33:39.944	X2/V100*(0)	X0	9.9.9.9	192.168.168.100	IP	ICMP	-	FORWARDED	74[74]
3	02/14/2007 13:33:39.944	-	X0*	9.9.9.9	192.168.168.100	IP	ICMP	-	FORWARDED	74[74]
4	02/14/2007 13:33:39.944	X0*(0)	X2/V100	192.168.168.100	9.9.9.9	IP	ICMP	-	FORWARDED	74[74]
5	02/14/2007 13:33:39.944	-	X2/V100*	192.168.168.100	9.9.9.9	IP	ICMP	-	FORWARDED	74[74]
6	02/14/2007 13:33:40.352	X0*(0)	X2/V100	192.168.168.100	9.9.9.9	IP	ICMP	-	FORWARDED	74[74]
7	02/14/2007 13:33:40.352	-	X2/V100*	192.168.168.100	9.9.9.9	IP	ICMP	-	FORWARDED	74[74]
8	02/14/2007 13:33:40.352	X2/V100*(0)	X0	9.9.9.9	192.168.168.100	IP	ICMP	-	FORWARDED	74[74]
9	02/14/2007 13:33:40.352	-	X0*	9.9.9.9	192.168.168.100	IP	ICMP	-	FORWARDED	74[74]

The UI also displays the buffer size, the number of packets captured, the percentage of buffer space used, and how much of the buffer has been lost. Lost packets occur when automatic FTP logging is turned on, but the file transfer is slow for some reason. If the transfer is not finished by the time the buffer is full again, the data in the newly filled buffer is lost.



#### Note

Although the buffer wrap option clears the buffer upon wrapping to the beginning, this is not considered lost data.

The FTP logging status indicator shows one of the following three conditions:

- Red: Automatic FTP logging is off
- Green: Automatic FTP logging is on
- Orange: The last attempt to contact the FTP server failed, and logging is now off

To restart automatic FTP logging, see [“Restarting FTP logging” on page 120](#).

Next to the FTP logging indicator, the UI also displays the number of successful and failed attempts to transfer the buffer contents to the FTP server, the current state of the FTP process thread, and the status of the capture buffer.

Under the FTP logging indicator, on the Current Buffer Statistics line, the UI displays the number of packets dropped, forwarded, consumed, generated, or unknown.

On the Current Configurations line, you can hover your mouse pointer over Filters, General, or Logging to view the currently configured value for each setting in that category. The Filters display includes the capture filter and display filter settings. The display for General includes both the general and advanced settings. The Logging display shows the FTP logging settings.

## Resetting the Status Information

You can reset the displayed statistics for the capture buffer and FTP logging. If a capture is in progress, it is not interrupted when you reset the statistics display.

- 
- Step 1** Navigate to the **Packet Capture** page in the UI.
- Step 2** Under **Packet Capture**, click **Reset**.

## Related Information

This section contains the following:

- [“Supported Packet Types” on page 122](#)
- [“File Formats for Export As” on page 122](#)

## Supported Packet Types

When specifying the Ethernet or IP packet types that you want to capture or display, you can use either the standard acronym for the type, if supported, or the corresponding hexadecimal representation. To determine the hex value for a protocol, refer to the RFC for the number assigned to it by IANA. The protocol acronyms that SonicOS Enhanced currently supports are as follows:

- Supported Ethernet types:
- ARP
  - IP
  - PPPoE-DIS
  - PPPoE-SES

To specify both PPPoE-DIS and PPPoE-SES, you can simply use PPPoE.

- Supported IP types:
- TCP
  - UDP
  - ICMP
  - IGMP
  - GRE
  - AH
  - ESP
- 

## File Formats for Export As

This section contains the following examples of the file formats available in the Export As option:

- [“HTML Format” on page 123](#)
- [“Text File Format” on page 124](#)

## HTML Format

You can view the HTML format in a browser. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 5.--

--990 packets captured.--

-----Statistics-----
Number Of Bytes Failed To Report:      0
Number Of Packets Forwarded           :      0
Number Of Packets Generated           :     250
Number Of Packets Consumed            :     140
Number Of Packets DROPPED             :     600
Number Of Packets Status Unknown:      0

*Packet number: 1*
Header Values:
  Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info (Time:08/29/2006 15:56:31.464):
  in:--, out:X0*, Generated (Sent Out)
Ethernet Header
  Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
  IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
  TCP Flags = [ACK,], Src=[80], Dst=[4712], Checksum=0xe425
Application Header
  HTTP
Value: [0]
Hex and ASCII dump of the packet:
00a0cc63 f0ab0006 b111a2ac 08004500 05dc05b0 00004006 *...c.....E.....@.*
9d0ec0a8 a8a8c0a8 a8640050 1268be1f 79d2b195 2ea35010 *.....d.P.h.y....P.*
2000e425 00003265 20373036 31363336 62203635 37343566 * ..%.2e 7061636b 65745f*
36332a5c 6e203230 32613633 36382036 35363432 30336120 *63*\n 202a6368 6564203a *
32303331 33623265 20326532 65326532 65203636 32653730 *20313b2e 2e2e2e2e 662e70*
36312036 33366236 35373420 2a202a63 68656420 3a20313b *61 636b6574 * *ched : 1; *
2e2e2e2e 2e662e70 61636b65 742a5c6e 20356636 33326135 *.....f.packet*\n 5f632a5*
```

## Text File Format

You can view the text format output in a text editor. The following is an example showing the header and part of the data for the first packet in the buffer.

```
--File Index : 7.--

--771 packets captured.--

-----Statistics-----
Number Of Bytes Failed To Report:      0
Number Of Packets Forwarded           :      0
Number Of Packets Generated            :     480
Number Of Packets Consumed             :     247
Number Of Packets DROPPED              :      44
Number Of Packets Status Unknown:      0

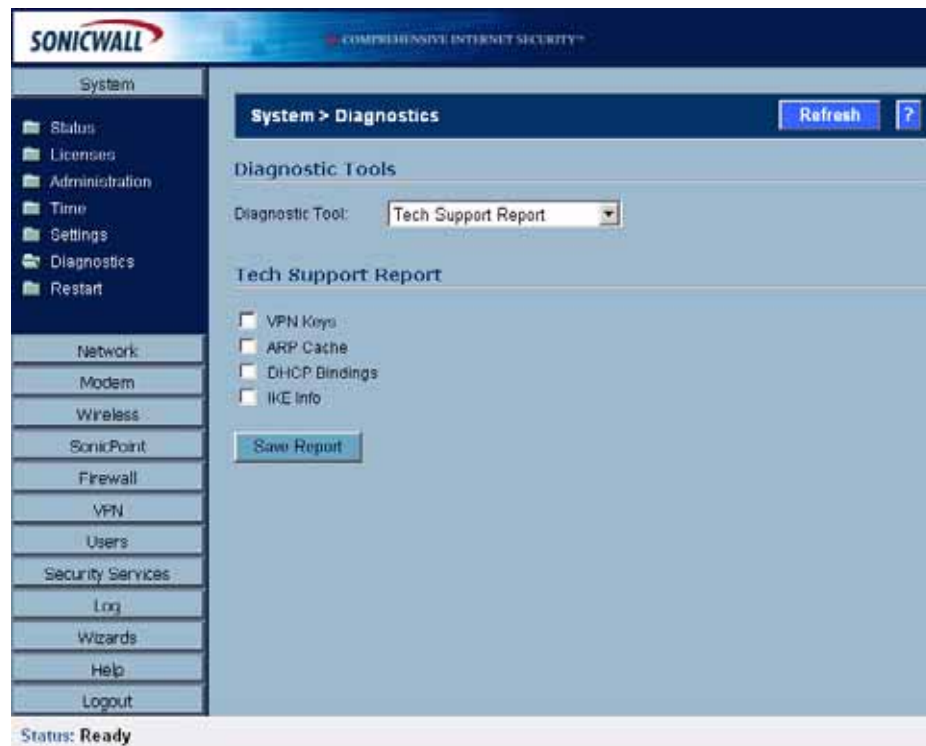
*Packet number: 1*
Header Values:
  Bytes captured: 1514, Actual Bytes on the wire: 60928
Packet Info(Time:08/29/2006 16:11:36.224):
  in:--, out:X0*, Generated (Sent Out)
Ethernet Header
  Ether Type: IP(0x800), Dst=[00:a0:cc:63:f0:ab], Src=[00:06:b1:11:a2:ac]
IP Packet Header
  IP Type: TCP(0x6), Src=[192.168.168.168], Dst=[192.168.168.100]
TCP Packet Header
  TCP Flags = [ACK,], Src=[80], Dst=[4763], Checksum=0xa1f
Application Header
  HTTP
Value:[0]
Hex and ASCII dump of the packet:
00a0cc63 f0ab0006 b111a2ac 08004500 05dc422e 00004006 *...c.....E...B...@.*
6090c0a8 a8a8c0a8 a8640050 129b4c70 07e7521d 0c005018 *`.....d.P..Lp..R...P.*
20000a1f 00006120 2a6e6420 666f7220 4e657462 696f732e * .....a *nd for Netbios.*
292c2028 4c696e65 3a2a0a20 32303336 33313337 20323034 *) , (Line:*. 20363137 204*
36373536 65203633 37343639 36662036 65336132 30363320 *6756e 6374696f 6e3a2063 *
37323635 36313734 20363534 65363537 34202a20 36313720 *72656174 654e6574 * 617 *
46756e63 74696f6e 3a206372 65617465 4e65742a 0a203632 *Function: createNet*. 62*
```

# CHAPTER 13

## Using Diagnostic Tools & Restarting the Appliance

### System > Diagnostics

The **System > Diagnostics** page provides several diagnostic tools which help troubleshoot network problems as well as Active Connections, CPU and Process Monitors.



## Tech Support Report

The **Tech Support Report** generates a detailed report of the SonicWALL security appliance configuration and status, and saves it to the local hard disk using the **Download Report** button. This file can then be e-mailed to SonicWALL Technical Support to help assist with a problem.



**Tip**

You must register your SonicWALL security appliance on [mySonicWALL.com](http://mySonicWALL.com) to receive technical support.

Before e-mailing the Tech Support Report to the SonicWALL Technical Support team, complete a Tech Support Request Form at <https://www.mysonicwall.com>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWALL Technical Support to provide you with better service.

### Generating a Tech Support Report



- Step 1** In the **Tech Support Report** section, select any of the following four report options:
- **VPN Keys** - saves shared secrets, encryption, and authentication keys to the report.
  - **ARP Cache** - saves a table relating IP addresses to the corresponding MAC or physical addresses.
  - **DHCP Bindings** - saves entries from the SonicWALL security appliance DHCP server.
  - **IKE Info** - saves current information about active IKE configurations.
- Step 2** Click **Download Report** to save the file to your system. When you click **Download Report**, a warning message is displayed.
- Step 3** Click **OK** to save the file. Attach the report to your **Tech Support Request** e-mail.



## Diagnostic Tools

You select the diagnostic tool from the **Diagnostic Tools** menu in the **Diagnostic Tool** section of the **System > Diagnostics** page. The following diagnostic tools are available:

- “Active Connections Monitor” on page 127
- “CPU Monitor” on page 128
- “DNS Name Lookup” on page 129
- “Find Network Path” on page 129
- “Packet Capture” on page 130
- “Ping” on page 131
- “Process Monitor” on page 132
- “Real-Time Black List Lookup” on page 132
- “Reverse Name Resolution” on page 132
- “Trace Route” on page 133
- “Web Server Monitor” on page 133

## Active Connections Monitor

The **Active Connections Monitor** displays real-time, exportable (plain text or CSV), filterable views of all connections to and through the SonicWALL security appliance. Click on a column heading to sort by that column.

Active Connections Monitor

Items 1 to 14 (of 14)

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.62	1849	192.168.168.168	443	TCP	WAN	LAN	1046	1592
2	10.0.202.62	1850	192.168.168.168	443	TCP	WAN	LAN	894	1508
3	10.0.202.62	1851	192.168.168.168	443	TCP	WAN	LAN	1358	2817
4	10.0.202.62	1852	192.168.168.168	443	TCP	WAN	LAN	374	310
5	10.0.202.62	1853	192.168.168.168	443	TCP	WAN	LAN	1354	11644
6	10.0.202.62	1854	192.168.168.168	443	TCP	WAN	LAN	1037	8571
7	10.0.202.62	1855	192.168.168.168	443	TCP	WAN	LAN	951	4943
8	10.0.202.62	1856	192.168.168.168	443	TCP	WAN	LAN	898	955
9	10.0.202.62	1857	192.168.168.168	443	TCP	WAN	LAN	1228	18125
10	10.0.202.62	1858	192.168.168.168	443	TCP	WAN	LAN	1080	8883
11	10.0.202.62	1859	192.168.168.168	443	TCP	WAN	LAN	943	2829
12	10.0.202.62	1860	192.168.168.168	443	TCP	WAN	LAN	1909	48179
13	10.0.202.62	1861	192.168.168.168	443	TCP	WAN	LAN	948	2511
14	10.0.202.62	1862	192.168.168.168	443	TCP	WAN	LAN	992	488

## Active Connections Monitor Settings

Active Connections Monitor Settings

Filter	Value	Group Filters
Source IP:	192.168.168.1	<input checked="" type="checkbox"/>
Destination IP:	10.0.93.31	<input checked="" type="checkbox"/>
Destination Port:		<input type="checkbox"/>
Protocol:	TCP(s)	<input type="checkbox"/>
Filter Logic:	(Source IP && Destination IP) && Destination Port && Protocol	

Apply Filters    Reset Filters    Export Results

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Protocol**, **Src Interface**, and **Dst Interface**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

*Source IP AND Destination IP*

Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

*(Source IP OR Destination IP) AND Protocol*

Click **Apply Filter** to apply the filter immediately to the **Active Connections Monitor** table. Click **Reset Filters** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.

## CPU Monitor

The **CPU Monitor** diagnostic tool shows real-time CPU utilization in second, minute, hour, and day intervals (historical data does not persist across reboots).



### Note

High CPU utilization is normal during Web-management page rendering, and while saving preferences to flash. Utilization by these tasks is an indication that available resources are being efficiently used rather than sitting idle. Traffic handling and other critical, performance-oriented and system tasks are always prioritized by the scheduler, and never experience starvation.



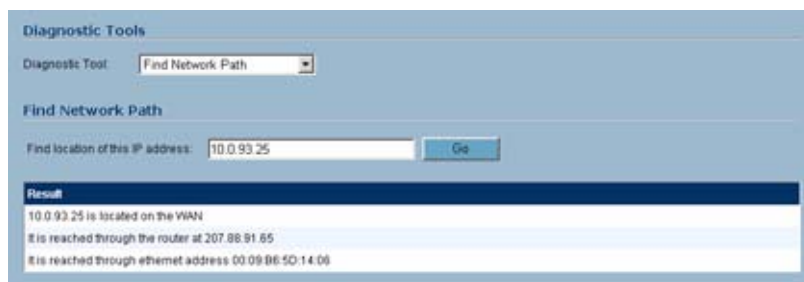
## DNS Name Lookup

The SonicWALL security appliance has a DNS lookup tool that returns the IP address of a domain name. Or, if you enter an IP address, it returns the domain name for that address.

- Step 1** Enter the host name or IP address in the **Look up name** field. Do not add *http* to the host name.
- Step 2** The SonicWALL security appliance queries the DNS Server and displays the result in the **Result** section. It also displays the IP address of the DNS Server used to perform the query.
- The **DNS Name Lookup** section also displays the IP addresses of the DNS Servers configured on the SonicWALL security appliance. If there is no IP address or IP addresses in the **DNS Server** fields, you must configure them on the **Network > Settings** page.

## Find Network Path

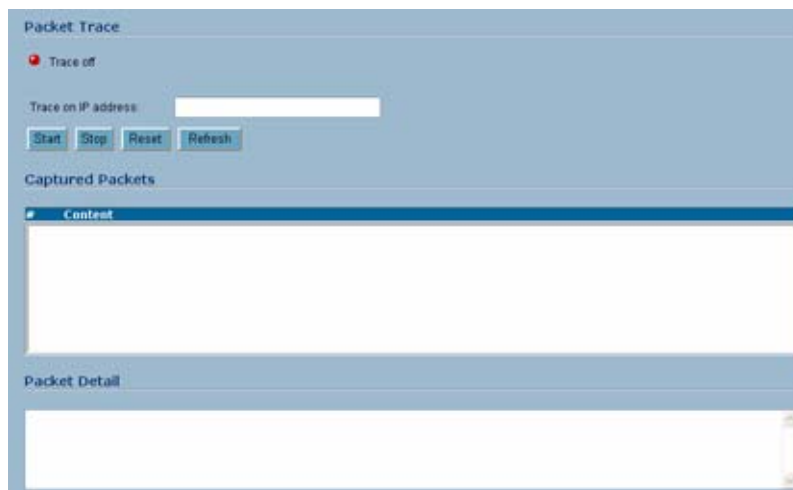
**Find Network Path** indicates if an IP host is located on the LAN or WAN ports. This can diagnose a network configuration problem on the SonicWALL security appliance. For example, if the SonicWALL security appliance indicates that a computer on the Internet is located on the LAN, then the network or Intranet settings may be misconfigured.



**Find Network Path** can be used to determine if a target device is located behind a network router and the Ethernet address of the target device. It also displays the gateway the device is using and helps isolate configuration problems.

## Packet Capture

The **Packet Capture** tool tracks the status of a communications stream as it moves from source to destination. This is a useful tool to determine if a communications stream is being stopped at the SonicWALL security appliance, or is lost on the Internet.



To interpret this tool, it is necessary to understand the three-way handshake that occurs for every TCP connection. The following displays a typical three-way handshake initiated by a host on the SonicWALL security appliance LAN to a remote host on the WAN.

- 
- Step 1** TCP received on LAN [SYN]  
**From** 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)  
**To** 204.71.200.74 / 80 (02:00:cf:58:d3:6a)  
 The SonicWALL security appliance receives SYN from LAN client.
- Step 2** TCP sent on WAN [SYN]  
**From** 207.88.211.116 / 1937 (00:40:10:0c:01:4e)  
**To** 204.71.200.74 / 80 (02:00:cf:58:d3:6a)  
 The SonicWALL security appliance forwards SYN from LAN client to remote host.
- Step 3** TCP received on WAN [SYN,ACK]  
**From** 204.71.200.74 / 80 (02:00:cf:58:d3:6a)  
**To** 207.88.211.116 / 1937 (00:40:10:0c:01:4e)  
 The SonicWALL security appliance receives SYN,ACK from remote host.
- Step 4** TCP sent on LAN [SYN,ACK]  
**From** 204.71.200.74 / 80 (02:00:cf:58:d3:6a)  
**To** 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)  
 The SonicWALL security appliance forwards SYN,ACK to LAN client.
- Step 5** TCP received on LAN [ACK]  
**From** 192.168.168.158 / 1282 (00:a0:4b:05:96:4a)  
**To** 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

Client sends a final ACK, and waits for start of data transfer.

- Step 6** TCP sent on WAN [ACK]  
**From** 207.88.211.116 / 1937 (00:40:10:0c:01:4e)  
**To** 204.71.200.74 / 80 (02:00:cf:58:d3:6a)

The SonicWALL security appliance forwards the client ACK to the remote host and waits for the data transfer to begin.

When using packet capture to isolate network connectivity problems, look for the location where the three-way handshake is breaking down. This helps to determine if the problem resides with the SonicWALL security appliance configuration, or if there is a problem on the Internet.

Select **Packet Capture** from the **Diagnostic tool** menu.



**Tip**

Packet Capture requires an IP address. The SonicWALL security appliance DNS Name Lookup tool can be used to find the IP address of a host.

- Step 7** Enter the IP address of the remote host in the **Trace on IP address** field, and click **Start**. You must enter an IP address in the **Trace on IP address** field; do not enter a host name, such as “www.yahoo.com”. The **Trace is off** turns from red to green with Trace Active displayed.
- Step 8** Contact the remote host using an IP application such as Web, FTP, or Telnet.
- Step 9** Click **Refresh** and the packet capture information is displayed.
- Step 10** Click **Stop** to terminate the packet capture, and **Reset** to clear the results.

The **Captured Packets** table displays the packet number and the content of the packet, for instance, *ARP Request send on WAN 42 bytes*.

Select a packet in the **Captured Packets** table to display packet details. Packet details include the packet number, time, content, source of the IP address, and the IP address destination.

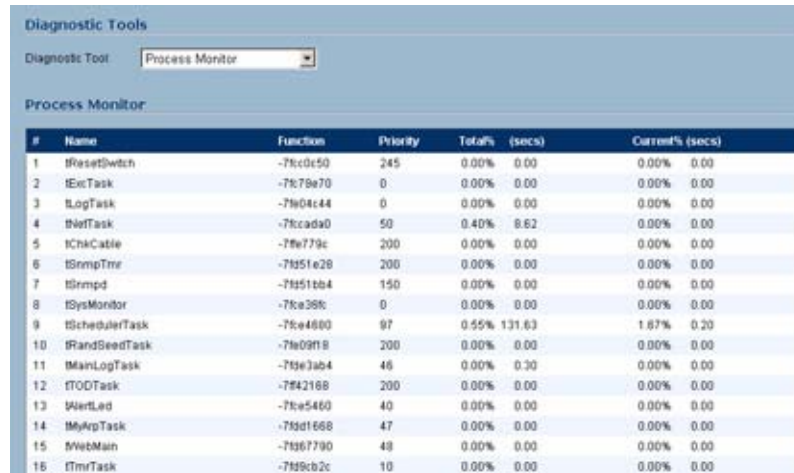
## Ping

The **Ping** test bounces a packet off a machine on the Internet and returns it to the sender. This test shows if the SonicWALL security appliance is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.

- Step 1** Select **Ping** from the **Diagnostic Tool** menu.
- Step 2** Enter the IP address or host name of the target device and click **Go**.
- Step 3** If the test is successful, the SonicWALL security appliance returns a message saying the IP address is alive and the time to return in milliseconds (ms).

## Process Monitor

**Process Monitor** shows individual system processes, their CPU utilization, and their system time.



Diagnostic Tools

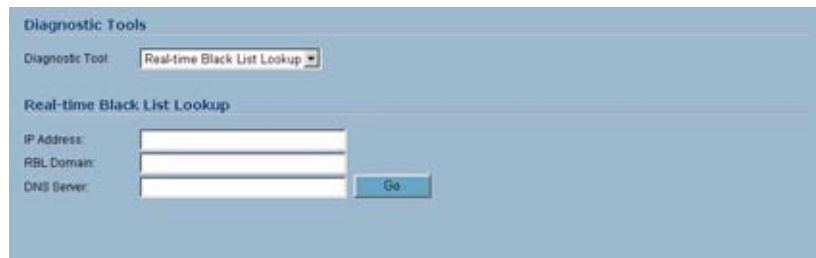
Diagnostic Tool: Process Monitor

Process Monitor

#	Name	Function	Priority	Total% (secs)	Current% (secs)
1	IRestSwitch	-7fc0e50	245	0.00%	0.00
2	IEicTask	-7fc79e70	0	0.00%	0.00
3	ILogTask	-7fe04c44	0	0.00%	0.00
4	INetTask	-7fccada0	50	0.40%	8.62
5	ICbkCable	-7fe779c	200	0.00%	0.00
6	ISnmpTrm	-7fd51e28	200	0.00%	0.00
7	ISnmpd	-7fd51bb4	150	0.00%	0.00
8	ISysMonitor	-7fc268c	0	0.00%	0.00
9	ISchedulerTask	-7fc4680	97	0.55%	131.63
10	IRandSeedTask	-7fe09f8	200	0.00%	0.00
11	MainLogTask	-7fe3ab4	46	0.00%	0.30
12	ITODTask	-7fd2188	200	0.00%	0.00
13	WartLed	-7fc5460	40	0.00%	0.00
14	IMyKpTask	-7fd1668	47	0.00%	0.00
15	MWebMain	-7fd7790	48	0.00%	0.00
16	ITmrTask	-7fd9cb2c	10	0.00%	0.00

## Real-Time Black List Lookup

The **Real-Time Black List Lookup** tool allows you to test SMTP IP addresses, RBL services, or DNS servers. Enter an IP address in the **IP Address** field, a FQDN for the RBL in the **RBL Domain** field and DNS server information in the **DNS Server** field. Click **Go**.



Diagnostic Tools

Diagnostic Tool: Real-time Black List Lookup

Real-time Black List Lookup

IP Address:

RBL Domain:

DNS Server:

## Reverse Name Resolution

The **Reverse Name Resolution** tool is similar to the DNS name lookup tool, except that it looks up a server name, given an IP address.



Diagnostic Tools

Diagnostic Tool: Reverse Name Resolution

Reverse Name Resolution

Log Resolution DNS Server 1:

Log Resolution DNS Server 2:

Log Resolution DNS Server 3:

Reverse Lookup the IP Address:

Enter an IP address in the **Reverse Lookup the IP Address** field, and it checks all DNS servers configured for your security appliance to resolve the IP address into a server name.

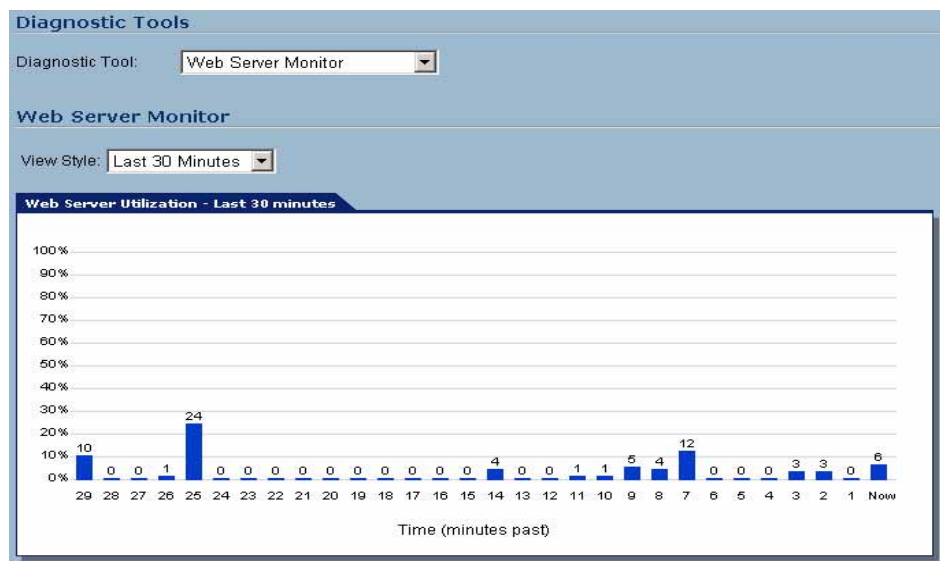
## Trace Route

**Trace Route** is a diagnostic utility to assist in diagnosing and troubleshooting router connections on the Internet. By using Internet Connect Message Protocol (ICMP) echo packets similar to Ping packets, **Trace Route** can test interconnectivity with routers and other hosts that are farther and farther along the network path until the connection fails or until the remote host responds.

Type the IP address or domain name of the destination host. For example, type yahoo.com and click **Go**. A second window is displayed with each hop to the destination host. By following the route, you can diagnose where the connection fails between the SonicWALL security appliance and the destination.

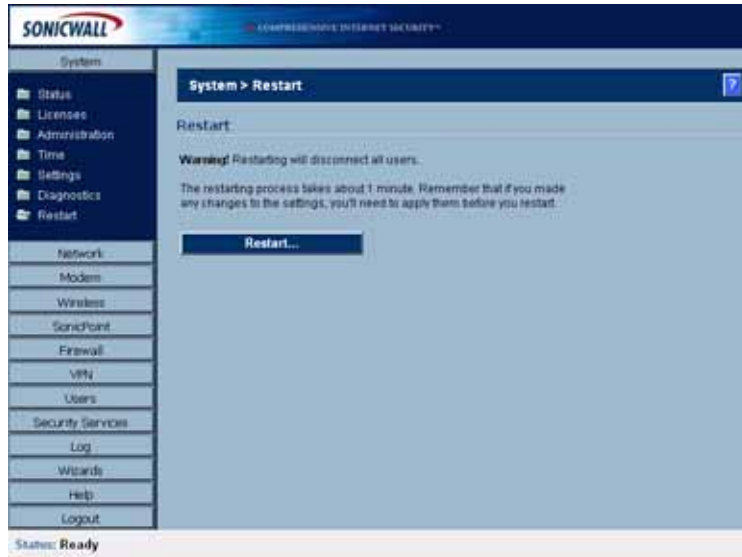
## Web Server Monitor

The **Web Server Monitor** tool displays the CPU utilization of the web server over several periods of time. The time frame of the Web Server Monitor can be changed by selecting one of the following options in the **View Style** pulldown menu: last 30 seconds, last 30 minutes, last 24 hours, or last 30 days.



## System > Restart

The SonicWALL security appliance can be restarted from the Web Management interface. Click **System > Restart** to display the Restart page.



Click **Restart...** and then click **Yes** to confirm the restart.

The SonicWALL security appliance takes approximately 60 seconds to restart, and the yellow Test light is lit during the restart. During the restart time, Internet access is momentarily interrupted on the LAN.

# **PART 3**

# **Network**





# CHAPTER 14

## Configuring Interfaces

### Network > Interfaces

The **Network > Interfaces** page includes interface objects that are directly linked to physical interfaces. The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. Physical interface objects include the LAN, WAN, and depending on which SonicWALL security appliance you have, OPT, Modem, WLAN, and WWAN ports in the SonicWALL security appliance.

**Network > Interfaces** [Wizards...](#) [Clear Statistics](#) [?](#)

**Interface Settings**

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
LAN	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
WAN	WAN	10.50.16.70	255.255.255.0	Static	100 Mbps full-duplex	Default WAN	
OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
WLAN	WLAN	172.16.31.1	255.255.255.0	Static	54 Mbps half-duplex	Default WLAN	
techpubs_test	WLAN	172.22.1.10	255.255.255.0	Static	WLAN Subnet		

[Add PortShield Interface](#) [Add WLAN Subnet](#)

**Interface Traffic Statistics**

Traffic Statistic	LAN	WAN	OPT	WLAN
Rx Unicast Packets:	297200	3209667	0	2404101
Rx Broadcast Packets:	9	63	0	0
Rx Bytes:	34925012	911212104	0	0
Tx Unicast Packets:	502422	336741	0	0
Tx Broadcast Packets:	155	945	0	0
Tx Bytes:	666339759	51139612	0	0

## Setup Wizard

The **Setup Wizard** button accesses the **Setup Wizard**. The Setup Wizard walks you through the configuration of the SonicWALL security appliance for Internet connectivity. For Setup Wizard instructions, see “[Wizards > Setup Wizard](#)” section on page 793.

## Interface Settings

The **Interface Settings** table lists the following information for each interface:

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
LAN	LAN	192.168.168.168	255.255.255.0	Static	No link	Default LAN	
WAN	WAN	10.50.16.70	255.255.255.0	Static	100 Mbps full-duplex	Default WAN	
OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		
WLAN	WLAN	172.16.31.1	255.255.255.0	Static	54 Mbps half-duplex	Default WLAN	
techpubs_test	WLAN	172.22.1.10	255.255.255.0	Static	WLAN Subnet		

- **Name** - Listed as **LAN**, **WAN**, **WWAN**, **WLAN**, or **OPT** depending on your SonicWALL security appliance model.
- **Zone** - LAN, DMZ/OPT, WAN, and WLAN are listed by default. As zones are configured, the names are listed in this column.
- **IP Address** - IP address assigned to the interface.
- **Subnet Mask** - the network mask assigned to the subnet.
- **IP Assignment** - you can select from the following options:
  - ◆ **LAN: Static or Transparent**
  - ◆ **WAN: DHCP, Static, PPPoE, PPTP, or L2TP**
  - ◆ **OPT:** The selection of IP assignment depends on the zone assigned to the user-defined port:
    - **LAN, DMZ**, or a custom zone of Trusted type: **Static or Transparent**
    - **WAN** or a custom zone of Untrusted type: **DHCP, Static, PPPoE, PPTP, or L2TP**
    - **WLAN** or a custom Wireless zone: static IPI only (no IP Assignment list)
  - ◆ **WLAN:** static IP only (no IP Assignment list)
- **Status** - The link status and speed.
- **Comment** - Any user-defined comments.
- **Configure** - Click the **Configure** icon to display the **Edit Interface** window, which allows you to configure the settings for the specified interface. Click the **trashcan** icon to delete a WLAN subnet.
- **Add PortShield Interface** - Click to create a PortShield interface. See “[Configuring SonicWALL PortShield Interfaces](#)” section on page 150 for more information.
- **Add WLAN Subnet** - Click to create a WLAN subnet to be used with a Virtual Access Point. See “[Creating a WLAN Subnet](#)” section on page 157 for more information.

**Caution** You cannot change the Zones in the Edit Interface window for the **LAN, WAN, Modem, and WLAN** interfaces.

## Interface Traffic Statistics

The **Interface Traffic Statistics** table lists received and transmitted information for all configured interfaces.

Interface Traffic Statistics						
Traffic Statistics	X0	X1	X2	X3	X4	X5
Rx Unicast Packets:	0	3947	0	0	0	0
Rx Broadcast Packets:	0	120920	0	0	0	0
Rx Bytes:	0	19095193	0	0	0	0
Tx Unicast Packets:	0	4755	0	0	0	0
Tx Broadcast Packets:	0	19	0	0	0	0
Tx Bytes:	0	3722726	0	0	0	0

The following information is displayed for all SonicWALL security appliance interfaces:

- **Rx Unicast Packets** - indicates the number of point-to-point communications received by the interface.
- **Rx Broadcast Packets** - indicates the number of multipoint communications received by the interface.
- **RX Bytes** - indicates the volume of data, in bytes, received by the interface.
- **Tx Unicast Packets** - indicates the number of point-to-point communications transmitted by the interface.
- **Tx Broadcast Bytes** - indicates the number of mutlipoint communications received by the interface.
- **Tx Bytes** - indicates the volume of data, in bytes, transmitted by the interface.

To clear the current statistics, click the **Clear Statistics** button at the top right of the **Network > Interfaces** page.



## Interfaces

Interfaces in SonicOS can be:

- **Physical interfaces:** Physical interfaces are bound to a single port
- **Virtual interfaces:** Virtual interfaces are assigned as sub-interfaces to a physical interface and allow the physical interface to carry traffic assigned to multiple interfaces.
- **PortShield interfaces:** PortShield interfaces allow for any of the LAN ports to be combined into single or multiple PortShield interfaces.

## Physical Interfaces

Physical interfaces must be assigned to a Zone to allow for configuration of Access Rules to govern inbound and outbound traffic. Security zones are bound to each physical interface where it acts as a conduit for inbound and outbound traffic. If there is no interface, traffic cannot access the zone or exit the zone.

For more information on zones, see [“Network > Zones” on page 191](#).

The first two interfaces, LAN and WAN are fixed interfaces, permanently bound to the Trusted and Untrusted Zone types. The TZ 170 series appliances can also have two special interfaces for Modem and WLAN. The remaining Interfaces can be configured and bound to any Zone type, depending on your SonicWALL security appliance.

## Permanently Assigned Interfaces

- SonicWALL TZ 170 and 180 series: **LAN** - The single LAN interface includes all five LAN ports on the back of the TZ 170 and 180 series appliances.
- SonicWALL TZ 190 Wireless: Wireless WAN (WWAN).

## User-definable Interfaces

- SonicWALL TZ 170, TZ 170 SP, TZ 180, and TZ 190 security appliances include one user definable interface, **OPT**.

## SonicOS Enhanced Secure Objects

The SonicOS Enhanced scheme of interface addressing works in conjunction with network zones and address objects. This structure is based on secure objects, which are utilized by rules and policies within SonicOS Enhanced. Physical interface objects include the LAN1 through LAN5, WAN, OPT, Modem and WLAN ports. Address objects comprise a host, a network, a range of addresses, or a MAC address.

Secured objects include interface objects that are directly linked to physical interfaces and managed in the **Network > Interfaces** page. Address objects are defined in the **Network > Address Objects** page. Service and Scheduling objects are defined in the **Firewall** section of the SonicWALL security appliance Management Interface, and User objects are defined in the **Users** section of the SonicWALL security appliance Management Interface.

Zones are the hierarchical apex of SonicOS Enhanced’s secure objects architecture. SonicOS Enhanced includes pre-defined zones as well as allow you to define your own zones. Predefined zones include LAN, DMZ, WAN, WLAN, and Custom. Zones can include multiple interfaces, however, the WAN Zone is restricted to a total of two interfaces. Within the WAN zone, either one or both WAN interfaces can be actively passing traffic depending on the WAN Failover and Load Balancing configuration on the **Network > WAN Failover & LB** page.

For more information on WAN Failover and Load Balancing on the SonicWALL security appliance, see Chapter 10 Setting Up Network WAN Failover and Load Balancing.

At the zone configuration level, the **Allow Interface Trust** setting for zones automates the processes involved in creating a permissive intra-zone Access Rule. It creates a comprehensive Address Object for the entire zone and a inclusively permissive Access Rule from zone address to zone addresses.

## Transparent Mode

Transparent Mode in SonicOS Enhanced uses interfaces as the top level of the management hierarchy. Transparent Mode supports unique addressing and interface routing.



## Configuring Interfaces

This section is divided into:

- [“Configuring the LAN and OPT Interfaces \(Static\)” on page 141](#)
- [“Configuring Advanced Settings for the Interface” on page 142](#)
- [“Configuring Interfaces in Transparent Mode” on page 143](#)
- [“Configuring Wireless Interfaces” on page 145](#)
- [“Configuring a WAN Interface” on page 147](#)
- [“Configuring SonicWALL PortShield Interfaces” on page 150](#)
- [“Creating a WLAN Subnet” section on page 157](#)

### Configuring the LAN and OPT Interfaces (Static)

Static means you assign a fixed IP address to the interface.

- Step 1** Click on the **Configure** icon  in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed.
- You can configure **F0, F1, X0** through **X9, LAN**, or **OPT**.
  - If you select **OPT**, select **LAN, WAN, DMZ, WLAN**, a custom zone, or **Create new zone** for **Zone**.
  - If you want to create a new zone, select **Create new zone**. The **Add Zone** window is displayed. See [“Network > Zones” section on page 191](#) for instructions on adding a zone.
- Step 2** Select a Zone to assign to the interface. You can select LAN, WAN, DMZ, WLAN, or a custom zone.
- Step 3** Select **Static** from the **IP Assignment** menu.
- Step 4** Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.
-  **Note** You cannot enter an IP address that is in the same subnet as another zone.
- Step 5** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 6** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP, HTTPS, SSH, Ping, SNMP**, and/or **SSH**.
- Step 7** If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 8** Click **OK**.

**Note**

The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance's address.

## Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.



The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

**Caution** If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.

## Configuring Interfaces in Transparent Mode

Transparent Mode enables the SonicWALL security appliance to bridge the WAN subnet onto an internal interface. You can configure the following interfaces in Transparent Mode:

- TZ family and PRO 1260: **Lan** and **Opt**
- PRO family: **X0, X2 - X9, F0**



**Note** You cannot configure the **X1** or **WAN** interface in Transparent mode.

To configure an interface for transparent mode, complete the following steps:

- Step 1** Click on the **Configure** icon in the **Configure** column for **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** Select an interface.
  - If you select a configurable interface, select **LAN** or **DMZ** for **Zone**.
  - If you want to create a new zone for the configurable interface, select **Create a new zone**. The **Add Zone** window is displayed. See [“Network > Zones” section on page 191](#) for instructions on adding a zone.
- Step 3** Select **Transparent Mode** from the **IP Assignment** menu.



- Step 4** From the **Transparent Range** menu, select an address object that contains the range of IP addresses you want to have access through this interface. The address range must be within the WAN zone and must not include the WAN interface IP address. If you do not have an address object configured that meets your needs:
  - a. In the **Transparent Range** menu, select **Create New Address Object**.
  - b. In the **Add Address Object** window, enter a name for the address range.
    - a. For **Zone Assignment**, select **WAN**
    - b. For **Type**, select:
      - **Host** if you want only one network device to connect to this interface.

- Range to specify a range of IP addresses by entering beginning and ending value of the range.
  - Network to specify a subnet by entering the beginning value and the subnet mask. The subnet must be within the WAN address range and cannot include the WAN interface IP address.
- c. Enter the IP address of the host, the beginning and ending address of the range, or the IP address and subnet mask of the network.
  - d. Click **OK** to create the address object and return to the **Edit Interface** window.

See “[Network > Address Objects](#)” section on page 203 for more information.

- Step 5** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 6** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
- Step 7** If you want to allow selected users with limited management rights to log directly into the security appliance through this interface, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 8** Click **OK**.



**Note** The administrator password is required to regenerate encryption keys after changing the SonicWALL security appliance’s address.

## Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex ( )
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.


Check **Enable Multicast Support** to allow multicast reception on this interface.

**Caution** If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.



## Configuring Wireless Interfaces

A Wireless interface is an interface that has been assigned to a Wireless zone and is used to support SonicWALL SonicPoint secure access points.

- Step 1** Click on the **Configure** icon  in the **Configure** column for the Interface you want to configure. The **Edit Interface** window is displayed. You can configure **X2** through **X9**, **Opt**, a VLAN sub-interface or a PortShield interface.
- Step 2** In the **Zone** list, select WLAN or a custom Wireless zone.
- Step 3** Enter the IP address and subnet mask of the Zone in the **IP Address** and **Subnet Mask** fields.



**Note** The upper limit of the subnet mask is determined by the number of SonicPoints you select in the SonicPoint Limit field. If you are configuring several interfaces or sub-interfaces as Wireless interfaces, you may want to use a smaller subnet (higher) to limit the number of potential DHCP leases available on the interface. Otherwise, if you use a class C subnet (subnet mask of 255.255.255.0) for each Wireless interface you may exceed the limit of DHCP leases available on the security appliance.

- Step 4** In the **SonicPoint Limit** field, select the maximum number of SonicPoints allowed on this interface.
- This value determines the highest subnet mask you can enter in the **Subnet Mask** field. The following table shows the subnet mask limit for each **SonicPoint Limit** selection and the number of DHCP leases available on the interface if you enter the maximum allowed subnet mask.
  - Available Client IPs assumes 1 IP for the SonicWALL gateway interface, in addition to the presence of the maximum number of SonicPoints allowed on this interface, each consuming an IP address.

SonicPoints per Interface	Maximum Subnet Mask	Total Usable IPs	Available Client IPs
No SonicPoints	30bits – 255.255.255.252	2	2
2 SonicPoints	29bits – 255.255.255.248	6	3
4 SonicPoints	29bits – 255.255.255.248	6	1
8 SonicPoints	28bits – 255.255.255.240	14	5
16 SonicPoints (PRO 4060, PRO 4100, and PRO 5060 only)	27bits – 255.255.255.224	30	13
32 SonicPoints (PRO 5060 only)	26bits – 255.255.255.192	62	29



**Note** The above table depicts the maximum subnet mask sizes allowed. You can still use class-full subnetting (class A, class B, or class C) or any variable length subnet mask that you wish on WLAN interfaces. You are encouraged to use a smaller subnet mask (e.g. 24bit class C - 255.255.255.0 - 254 total usable IPs), thus allocating more IP addressing space to clients if you have the need to support larger numbers of wireless clients.

- Step 5** Enter any optional comment text in the **Comment** field. This text is displayed in the **Comment** column of the **Interface** table.
- Step 6** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**.
- Step 7** If you want to allow selected users with limited management rights to log in to the security appliance, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 8** Click **OK**.

## Configuring Advanced Settings for the Interface

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab.



The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 1000 Mbps - Full Duplex
- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

**Caution** If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL security appliance as well.

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

Check **Enable Multicast Support** to allow multicast reception on this interface.

Check **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see [“Firewall > QoS Mapping” section on page 467](#).

## Configuring a WAN Interface

Configuring the WAN interface enables Internet connect connectivity. You can configure up to two WAN interfaces on the SonicWALL security appliance.

- Step 1** Click on the **Notepad** icon in the **Configure** column for the **F1, WAN, X1** or **Unassigned** Interface you want to configure. The **Edit Interface** window is displayed.
- Step 2** If you're configuring an Unassigned Interface, select **WAN** from the **Zone** menu. If you selected the **Default WAN** Interface, **WAN** is already selected in the **Zone** menu.



- Step 3** Select one of the following WAN Network Addressing Mode from the **IP Assignment** menu. Depending on the option you choose from the IP Assignment menu, complete the corresponding fields that are displayed after selecting the option.
- **Static** - configures the SonicWALL for a network that uses static IP addresses.

- **DHCP** - configures the SonicWALL to request IP settings from a DHCP server on the Internet. NAT with DHCP Client is a typical network addressing mode for cable and DSL customers.
- **PPPoE** - uses Point to Point Protocol over Ethernet (PPPoE) to connect to the Internet. If desktop software and a username and password is required by your ISP, select NAT with PPPoE. This protocol is typically found when using a DSL modem.
- **PPTP** - uses PPTP (Point to Point Tunneling Protocol) to connect to a remote server. It supports older Microsoft Windows implementations requiring tunneling connectivity.
- **L2TP** - uses IPsec to connect a L2TP (Layer 2 Tunneling Protocol) server and encrypts all data transmitted from the client to the server. However, it does not encrypt network traffic to other destinations.

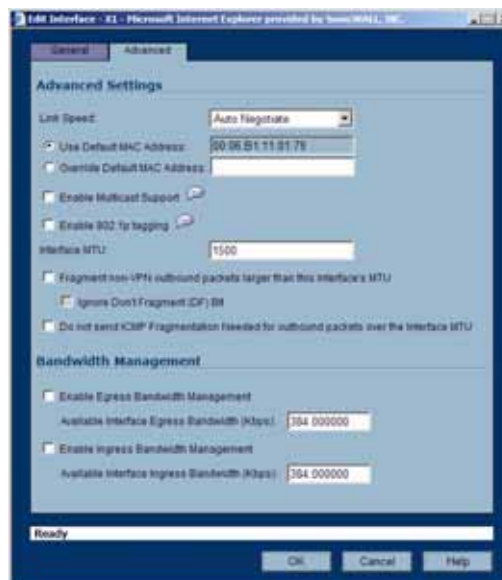


**Note** For Windows clients, L2TP is supported by Windows 2000 and Windows XP. If you are running other versions of Windows, you must use PPTP as your tunneling protocol.

- Step 4** If you want to enable remote management of the SonicWALL security appliance from this interface, select the supported management protocol(s): **HTTP**, **HTTPS**, **SSH**, **Ping**, **SNMP**, and/or **SSH**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.
- Step 5** If you want to allow selected users with limited management rights to log directly into the security appliance from this interface, select **HTTP** and/or **HTTPS** in **User Login**.
- Step 6** Check **Add rule to enable redirect from HTTP to HTTPS**, if you want an HTTP connection automatically redirected to a secure HTTPS connection to the SonicWALL security appliance management interface.
- Step 7** After completing the WAN configuration for your Network Addressing Mode, click **OK**

## Configuring the Advanced Settings for the WAN Interface

The **Advanced** tab includes settings for forcing an Ethernet speed and duplex, overriding the Default MAC Address, setting up bandwidth management, and creating a default NAT policy automatically.



## Ethernet Settings

If you need to force an Ethernet speed, duplex and/or MAC address, click the **Advanced** tab. The **Ethernet Settings** section allows you to manage the Ethernet settings of links connected to the SonicWALL. **Auto Negotiate** is selected by default as the **Link Speed** because the Ethernet links automatically negotiate the speed and duplex mode of the Ethernet connection. If you want to specify the forced Ethernet speed and duplex, select one of the following options from the **Link Speed** menu:

- 100 Mbps - Full Duplex
- 100 Mbps - Half Duplex
- 10 Mbps - Full Duplex
- 10 Mbps - Half Duplex

You can choose to override the **Default MAC Address** for the Interface by selecting **Override Default MAC Address** and entering the MAC Address in the field.

---

**Caution** If you select a specific Ethernet speed and duplex, you must force the connection speed and duplex from the Ethernet card to the SonicWALL as well.

---

Check **Enable Multicast Support** to allow multicast reception on this interface.

Check **Enable 802.1p tagging** to tag information passing through this interface with 802.1p priority information for Quality of Service (QoS) management. Packets sent through this interface are tagged with VLAN id=0 and carry 802.1p priority information. In order to make use of this priority information, devices connected to this interface should support priority frames. QoS management is controlled by access rules on the **Firewall > Access Rules** page. For information on QoS and bandwidth management, see [“Firewall > QoS Mapping” section on page 467](#).

You can also specify any of these additional **Ethernet Settings**:

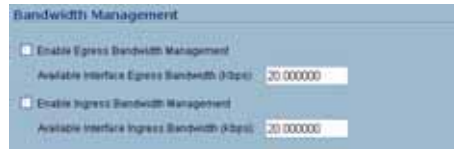
- **Interface MTU** - Specifies the largest packet size that the interface can forward without fragmenting the packet.
- **Fragment non-VPN outbound packets larger than this Interface’s MTU** - Specifies all non-VPN outbound packets larger than this Interface’s MTU be fragmented. Specifying the fragmenting of VPN outbound packets is set in the **VPN > Advanced** page.
- **Ignore Don’t Fragment (DF) Bit** - Overrides DF bits in packets.
- **Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU** - blocks notification that this interface can receive fragmented packets.

## Bandwidth Management

SonicOS Enhanced can apply bandwidth management to both egress (outbound) and ingress (inbound) traffic on the WAN interface. Outbound bandwidth management is done using Class Based Queuing. Inbound Bandwidth Management is done by implementing ACK delay algorithm that uses TCP’s intrinsic behavior to control the traffic.

Class Based Queuing (CBQ) provides guaranteed and maximum bandwidth Quality of Service (QoS) for the SonicWALL security appliance. Every packet destined to the WAN interface is queued in the corresponding priority queue. The scheduler then dequeues the packets and transmits it on the link depending on the guaranteed bandwidth for the flow and the available link bandwidth.

Use the Bandwidth Management section of the **Edit Interface** screen to enable or disable the ingress and egress bandwidth management. Egress and Ingress available link bandwidth can be used to configure the upstream and downstream connection speeds.



The **Bandwidth Management** section allows you to specify the available outbound bandwidth for this interface in Kbps.

- **Enable Egress Bandwidth Management** - Enables outbound bandwidth management.
  - **Available Interface Egress Bandwidth (Kbps)** - Specifies the available bandwidth for this interface in Kbps.
- **Enable Ingress Bandwidth Management** - Enables inbound bandwidth management.
  - **Available Interface Ingress Bandwidth (Kbps)** - Specifies the available bandwidth for this interface in Kbps.

## NAT Policy Settings

Selecting **Create default NAT Policy automatically** translates the Source Address of packets from the **Default LAN** (Primary LAN) to your new **WAN** Interface.

For more information on NAT Policies, see Chapter 15 Configuring Network NAT Policies.

## Configuring SonicWALL PortShield Interfaces

SonicWALL PortShield™ is a feature of the SonicWALL PRO 1260 security appliance running SonicOS Enhanced 3.1 or newer and the SonicWALL TZ 180 and TZ 190 running SonicOS Enhanced 3.6 or newer..

PortShield architecture enables you to configure any or all of the LAN switch ports on the into separate security zones, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each security zone has its own wire-speed switch ports that enjoy the protection of a dedicated, deep packet inspection firewall.

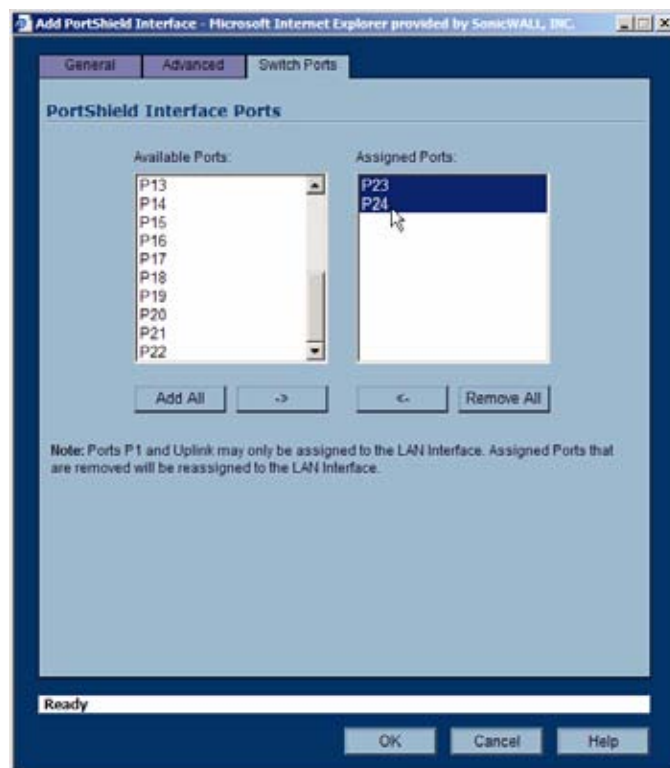
To add a PortShield interface, perform the following steps:

- 
- Step 1** In the **Network > Interfaces** page, click **Add PortShield Interface**.
- Step 2** Configure the following options interface:
- **Zone:** The zone assigned to this interface
  - **PortShield Interface Name:** The name of the interface
  - **IP Address:** An appropriate IP address that does not conflict with another address range.

- **Subnet Mask:** 255.255.255.0 is the default



**Step 3** In the **Switch Ports** tab, chose which ports to add to the PortShield interface.



## Configuring the Wireless WAN Interface

The SonicWALL TZ 190 security appliance introduces support for 3G (third generation) Wireless WAN connections that utilize data connections over 3G cellular networks. The Wireless WAN (WWAN) can be used for:

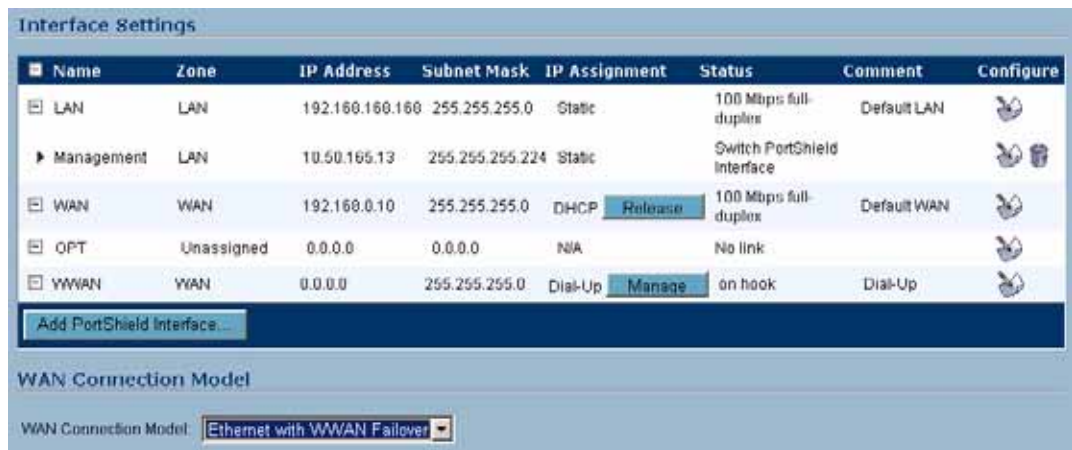
- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a pre-configured connection may not be available, such as trade-shows and kiosks.
- Mobile networks, where the SonicWALL TZ 190 is based in a vehicle.
- Primary WAN connection where wire-based connections are not available and 3G cellular is.

Most WWAN settings can be configured on the **Network > Interfaces** page. To configure WWAN connection profiles, you must use the **WWAN > Connection Profiles** page. For more information, see **Chapter 32, Configuring Wireless WAN**. This chapter also contains more information on Wireless WAN in general and the specifics of SonicWALL’s WWAN implementation.

The following sections describe how to configure the Wireless WAN interface:

- [“Managing WWAN Connections” on page 153](#)
- [“Specifying the WAN Connection Model” on page 153](#)
- [“Configuring Basic Wireless WAN Settings” on page 154](#)
- [“Configuring Remotely Triggered Dial-Out on the WWAN” on page 156](#)
- [“Configuring the Maximum Allowed WWAN Connections” on page 157](#)

On the SonicWALL TZ 190, the WWAN interface is the last listed interface in the **interface Settings** section of the **Network > Interfaces** page.





## Managing WWAN Connections

To initiate a WWAN connection, on the **Network > Interfaces** page, click on the **Manage** button in the **WWAN** interface line. The **WWAN Connection** window displays. Click the **Connect** button. The SonicWALL TZ 190 attempts to connect to the WWAN service provider.



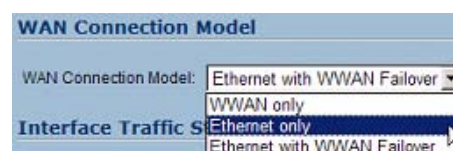
To disconnect a WWAN connection, click on the **Manage** button. The **WWAN Connection** window displays. Click **Disconnect**.



## Specifying the WAN Connection Model

To configure the WAN connection model, navigate to the **Network > Interfaces** page and select one of the following options in the **WAN Connection Model** pull-down menu:

- **WWAN only** - The WAN interface is disabled and the WWAN interface is used exclusively.
- **Ethernet only** - The WWAN interface is disabled and the WAN interface is used exclusively.
- **Ethernet with WWAN Failover** - The WAN interface is used as the primary interface and the WWAN interface is disabled. If the WAN connection fails, the WWAN interface is enabled and a WWAN connection is automatically initiated.

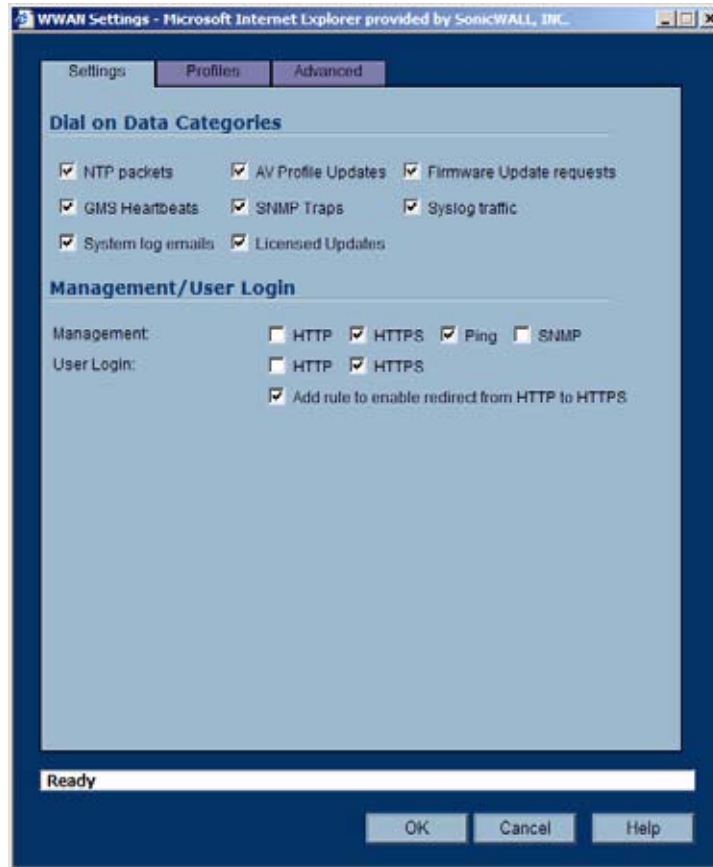


For a detailed explanation of the behavior of the **Ethernet with WWAN Failover** setting refer to “Understanding Wireless WAN Connection Models” on page 274.

## Configuring Basic Wireless WAN Settings

To configure basic WWAN interface settings, perform the following steps:

- Step 1** Click the edit icon  for the WWAN interface. The **WWAN Settings** window is displayed.



- Step 2** To configure the WWAN interface to automatically connect to the WWAN service provider when the SonicWALL TZ 190 detects specific types of traffic, select the appropriate categories in the **Dial on Data Categories** section.



**Note** To configure the SonicWALL TZ 190 for Connect on Data operation, you must select **Dial on Data** as the **Dial Type** for the Connection Profile. See “**Configuring WWAN Connection Profiles**” on page 283 in **Chapter 32, Configuring Wireless WAN** for more details.

- Step 3** Select which protocols can be used for administrators and users to log in to the SonicWALL TZ 190 appliance over the WWAN interface in the **Management/User Login** section must be configure to enable remote management of the SonicWALL TZ 190 appliance over the WWAN interface.
- Step 4** Select **Add rule to enable redirect from HTTP to HTTPS** to allow the SonicWALL to automatically convert HTTP requests to HTTPS requests for added security. Bear in mind that HTTP traffic is less secure than HTTPS.
- Step 5** Click on the **Profiles** tab.



- Step 6** Select the Primary WWAN connection profile in the **Primary Profile** pull-down menu. Optionally, you can select up to two alternate WWAN profiles.



**Note** WWAN connection profiles are configured on the **WWAN > Connection Profiles** page. For more information, see “**Configuring WWAN Connection Profiles**” on page 283 in **Chapter 32, Configuring Wireless WAN** for more details.

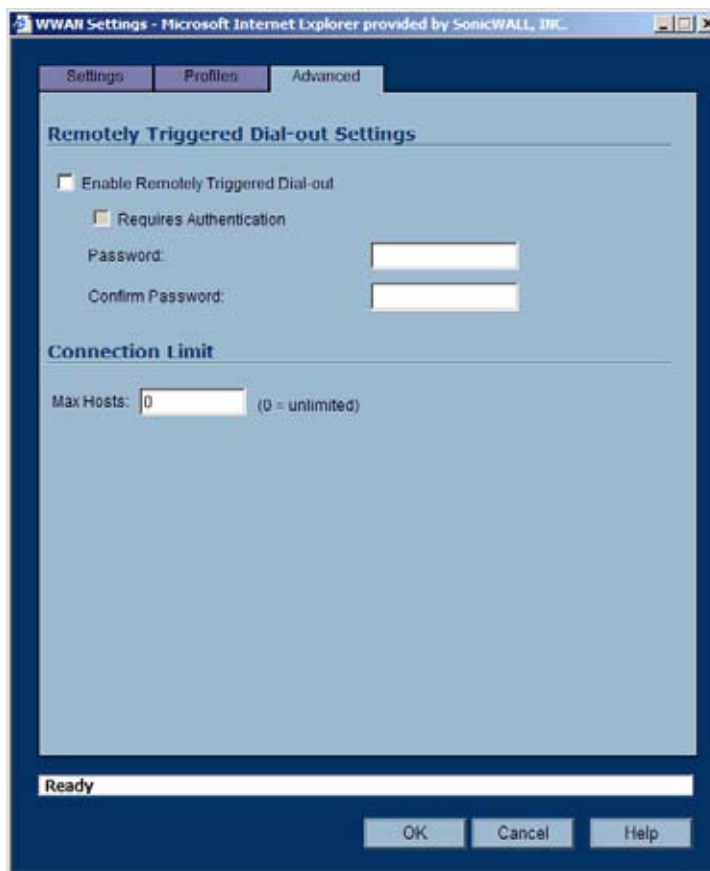
## Configuring Remotely Triggered Dial-Out on the WWAN

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The WWAN profile is configured for **dial-on-data**.
- The SonicWALL Security Appliance is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Max Connection Time (minutes)** field. This field is located in the **WWAN Profile Configuration** window on the **Parameters** tab. See “*Configuring WWAN Connection Profiles*” on page 283 in **Chapter 32, Configuring Wireless WAN** for more information. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

To enable remotely triggered dial-out over the WWAN interface, perform the following steps:

- Step 1** Click on the **Advanced** tab of the **WWAN Settings** window.



- Step 2** To enable network administrators to remotely initiate a WWAN connection from a SonicWALL TZ 190, select the **Enable Remotely Triggered Dial-out** checkbox.
- Step 3** To require remotely triggered dial-out sessions to be authenticated, select the **Requires Authentication** checkbox and enter a password in the **Password** and **Confirm Password** fields.

## Configuring the Maximum Allowed WWAN Connections

To configure the maximum number of nodes allowed to connect to the WWAN interface, enter the maximum number of nodes in the **Max Host** field. Entering **0** in the **Max Host** fields allows any number of nodes to connect.

## Creating a WLAN Subnet

WLAN subnets are used to segment IP address space for use by Virtual Access Points (VAP). Each VAP must have a separate WLAN subnet, and you must create the WLAN subnet before creating the VAP. To create a WLAN subnet, complete the following steps.

**Step 1** On the **Network > Interfaces** page, click the **Add WLAN Subnet** button.

**Step 2** Configure the following options:

- **Zone:** By default, the zone is set to **WLAN**. You can select any other wireless zone that you have created on the **Network > Zones** page.
- **Subnet Name:** The name of the interface.
- **IP Address:** The first IP address in the subnet. Make sure that the IP address subnet does not conflict with another address range.
- **Subnet Mask:** 255.255.255.0 is the default

- **SonicPoint Limit:** The maximum number of allowed SonicPoints is configured automatically.
- **Comment:** Optionally enter a comment about the subnet.
- **Management:** Select the appropriate protocols to allow remote management of the SonicWALL security appliance from this subnet.
- **User Login:** Select **HTTP** and/or **HTTPS** to allow users with limited management rights to log in to the SonicWALL security appliance.
- **Add rule to enable redirect from HTTP to HTTPS:** If you select **HTTPS** but do not select **HTTP** for either **Management** or **User Login**, select this option to redirect HTTP users to HTTPS.
- **Create default DHCP Lease Scope:** Select to create a DHCP lease scope for this subnet. The DHCP lease scope consists of the IP addresses that are reserved for users who connect to the VAP associated with this WLAN subnet. This option is enabled by default.

To configure additional options for the DHCP lease scope (such as the number of IP addresses and the lease time), go to the **Network > DHCP Server** page, locate the lease scope in the DHCP Server Lease Scope table, and click on the **Configure** icon. See [“Network > DHCP Server” section on page 277](#) for more information.

**Step 3** Optionally, you can enable multicast reception on the subnet by clicking on the **Advanced** tab and selecting the **Enable multicast support** checkbox.

**Step 4** Click **OK**.



## CHAPTER 15

# Configuring PortShield Interfaces

---

## SonicWALL PortShield Interfaces

SonicWALL PortShield is a feature of the SonicWALL TZ 180 and TZ 190 security appliances running SonicOS Enhanced 3.8 or newer.

PortShield architecture enables you to configure some or all of the LAN switch ports on the TZ 180 and TZ 190 into separate security contexts, providing protection not only from the WAN and DMZ, but between devices inside your network as well. In effect, each context has its own wire-speed switch ports that enjoy the protection of a dedicated, deep packet inspection firewall. The SonicWALL TZ 180 has five switch ports, and the SonicWALL TZ 190 has eight switch ports.

**Note**

---

Port 1 and the Uplink port are the only ports from which you can establish a SonicOS management session with the device.

---

You can assign any combination of ports into a PortShield interface. All ports you do not assign to a PortShield interface are assigned to the LAN interface. For example, on a SonicWALL TZ 190 if you assign ports 4 through 8 to a PortShield interface, ports 1 through 3 and the uplink port are all assigned to the LAN interface.

**Note**

---

Port 1 and the Uplink port can not be assigned to a PortShield interface. They can only be LAN interface. The OPT and WAN ports can not be assigned to a PortShield interface.

---

## Security Services with PortShield

When you enable SonicWALL Security Services, such as Gateway Anti-Virus (GAV), Anti-Spyware, and Intrusion Prevention Service (IPS), the services inspect traffic between different PortShield interfaces and not traffic between ports within the same PortShield interface.

For example, if ports 2 and 3 are assigned to the SwitchPort1 interface and ports 4 and 5 are assigned to the SwitchPort2 interface, traffic between port 2 and port 3 will not be inspected by Security Services. Traffic between port 2 and port 4 will be inspected.

## Network > SwitchPorts

The **Network > SwitchPorts** page allows you to manage the assignments of ports to PortShield interfaces.

Name	PortShield Interface	Link Settings	Link Status	Comment	Configure
1	LAN	Auto Negotiate	No link		
2	PortShield Interface 1	Auto Negotiate	No link		
3	PortShield Interface 2	Auto Negotiate	No link		
4	PortShield Interface 3	Auto Negotiate	No link		
5	LAN	Auto Negotiate	No link		

## Overview

A PortShield interface is a virtual interface with a set of ports assigned to it. There are two IP assignment methods you can deploy to create PortShield interfaces. They are Static and Transparent modes. The following two sections describe each.

### Working in Static Mode

When you create a PortShield interface in Static Mode, you manually create an explicit address to be applied to the PortShield interface. All ports mapped to the interface are identified by this address. Static mode is available on interfaces assigned to Trusted, Public, or Wireless zones.



**Note**

When you create a PortShield interface in Static Mode, make sure the IP address you assign to the interface is not already in use by another PortShield interface.

### Working in Transparent Mode

Transparent Mode addressing allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address is the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.



**Note**

Make sure the IP address you assign to the PortShield interface is within the WAN subnetwork.



When you create a PortShield interface in Transparent Mode, you create a range of addresses to be applied to the PortShield interface. You include these addresses in one entity called an Address Object. Address Objects allow for entities to be defined one time and to be re-used in multiple referential instances throughout the SonicOS interface. When you create a PortShield interface using an address object, all ports mapped to the interface are identified by any of the addresses specified in the address range.



**Note**

Each statically addressed PortShield interface must be on a unique subnet. You can not overlap PortShield interfaces across multiple subnetworks.

## Using Different Approaches to Configuration

There are four ways to approach configuration of PortShield interface. They are:

- By going into the Interfaces environment and clicking the **Add PortShield Interface** button.
- By going into the Switch Ports environment and clicking on port icons in an interactive graphic of the SonicWALL TZ 180 or TZ 190 appliance.
- By going into the Switch Ports environment and clicking on the pen and paper icon in the Configure column of the switch ports list.
- By using the PortShield interface wizard and clicking on options presented in the wizard screens.

To create a PortShield interface using the first method, perform the following tasks:

1. Log into the SonicWALL TZ 180 or TZ 190 security appliance.
2. Create and add a PortShield interface to the list of interfaces. The PortShield interface is a virtual interface that you are adding to segment and control traffic for the 8-port managed SonicWALL TZ 180 or TZ 190 appliance. After you select a zone, you select a series of ports that you want to assign to the PortShield interface.
3. Navigate to the Switch Port environment and perform either per-port or multiple-port extra configuration.

To create a PortShield interface using the second and third methods, perform the following tasks:

1. Log into the SonicWALL TZ 180 or TZ 190 security appliance.
2. Create and add a PortShield interface to the list of interfaces.
3. Go to the Switch Port environment and assign ports to the PortShield interface you have already created.
  - For the second method, select ports from the device graphic.
  - For third method, click on the pen and paper icon and select ports from the same dialog boxes you work in the Interface environment.
4. Perform per-port or multiple-port extra configuration.

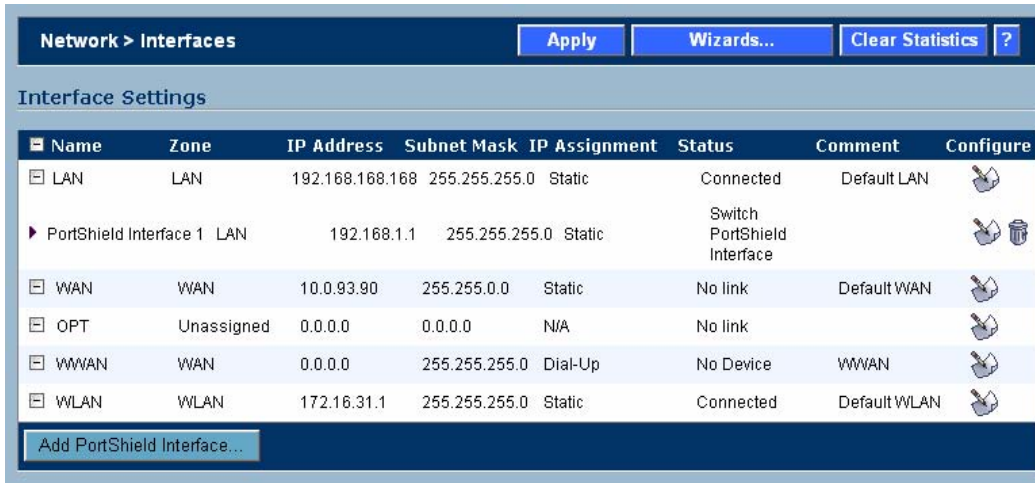
To create a PortShield interface using the fourth method, perform the following tasks:

1. Log into the SonicWALL TZ 180 or TZ 190 security appliance.
2. Click **Wizards** environment and select the **PortShield Interface Wizard**.
3. Navigate through the wizard screens, selecting and verifying one of the options presented for switch partitioning which divides the ports up into various amounts.

## Creating a PortShield Interface from the Interfaces Area

Before creating and adding a PortShield interface, think about why you are creating it and what role it will play in your network. To create and add a PortShield interface to the list of interfaces, perform the following steps:

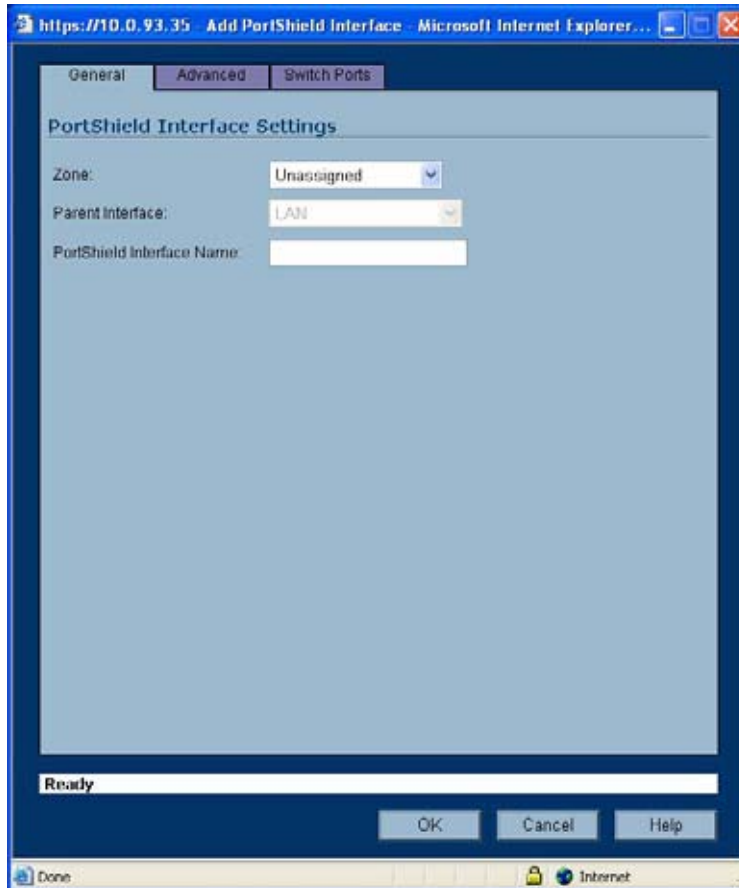
- Click on the **Network > Interfaces** page.



- The interfaces in the list contain the following information:

Column	Description
Name	A string that identifies the interface.
Zone	The zone to which the interface maps.
IP Address	The IP address assigned to the interface.
Subnet Mask	The subnetwork mask value assigned to the IP address to indicate a range of addresses.
IP Assignment	The method in which the interface obtains its IP address: <ul style="list-style-type: none"> <li><b>Static.</b> Manually creating an explicit address to which you will map ports.</li> <li><b>Transparent.</b> Allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address will be the same as the WAN interface IP address. Transparent mode is available on interfaces assigned to Trusted and Public Zones.</li> </ul>
Status	Aggregate Ethernet Link port(s) status or Ethernet Link port(s) status summary, indicating the currently active highest speed and duplex properties.
Comment	A note about the interface.
Configure	Contains two icons. One icon is a grouping of books that displays traffic statistics when you hover the mouse cursor over it. The other icon is a pen and paper that enables you to launch an interface configuration session.

- Click the **Add PortShield Interface** button. The Add Port Shield dialog box displays.



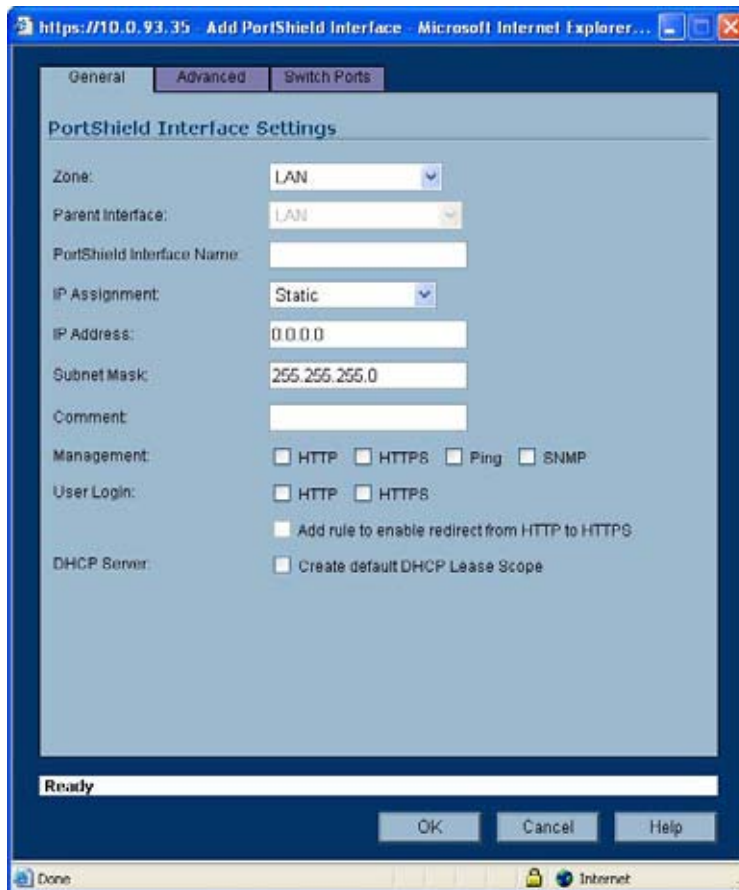
- Click the **Zone** list box and click on a zone type option to which you want to map the interface. Default zones are:
  - LAN
  - DMZ
  - WLAN
  - Unassigned

If you want to create another zone, go to the section “Creating a New Zone for the PortShield Interface” on page 166.

**Note**

You can add PortShield interfaces only to Trusted, Public, and Wireless zones.

8. After you select a zone option, the management software displays a more expanded version of the PortShield Interface Settings dialog box.

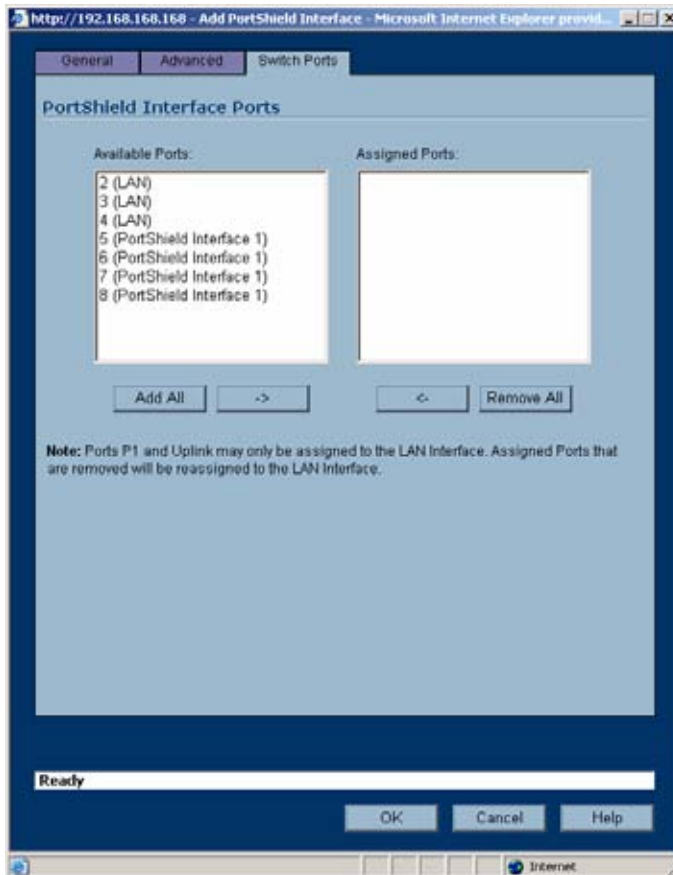


9. Type a string in the **PortShield Interface Name** field.
10. Click on the **IP Assignment** list box and select either **Static** or **Transparent**. Static indicates the interface obtains its IP address manually. Transparent mode allows for the WAN subnetwork to be shared by the current interface using Address Object assignments. The interface's IP address will be the same as the WAN interface IP address.
11. Type an available IP address in the **IP Address** field.
12. If you want to specify a range of IP addresses different than the one allowed by the subnetwork mask 255.255.255.0 (Class C network), type in the desired subnetwork mask value in the **Subnet Mask** field.
13. Click on a checkbox in the Management area to indicate the desired management protocol type. The options are:
  - HTTP
  - HTTPS
  - Ping
  - SNMP
14. Click on a checkbox in the User Login area. This is a special feature that enables you to set up a Web access environment so you can enforce User Level Authentication.
15. Click on the Create Default DHCP Lease Scope in the DHCP Server field to indicate that the amount of time allowed for an IP address issued by DHCP will be the default.

**Note**

This option only appears when creating a PortShield interface, not when editing an existing PortShield interface. You can make changes to the interface's DHCP settings after creating an interface from the DHCP Server environment (**Network > DHCP Server**).

- Click on the **Switch Ports** tab. The management software displays the PortShield Interface dialog box.

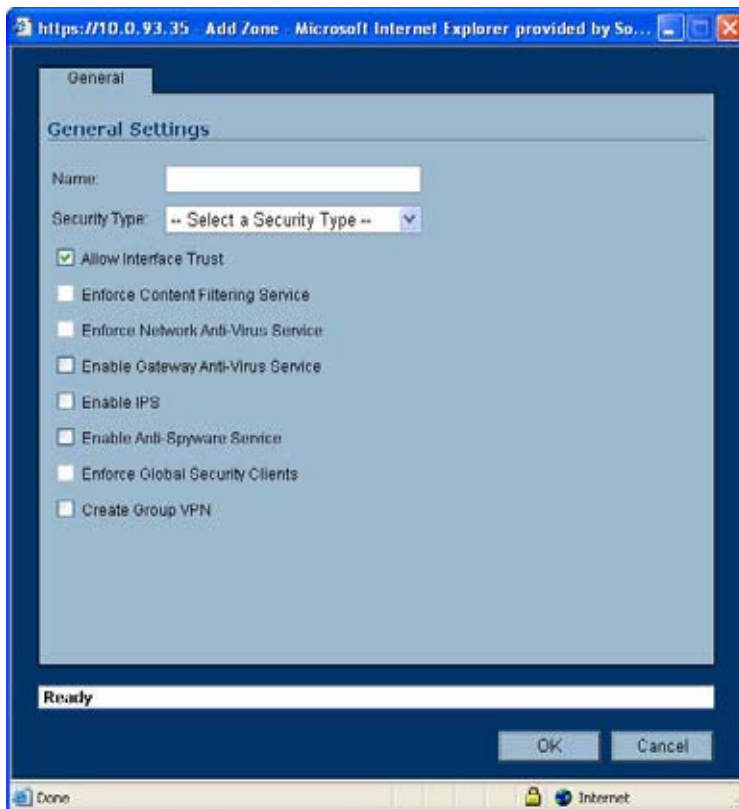


- In the **Available Ports** list, click on the port numbers you want to assign to the PortShield interface and click on the right arrow (>) button to move them into the Assigned Ports list.
- Click **OK**. The management software adds the PortShield interface to the interface list.

## Creating a New Zone for the PortShield Interface

You may want to create a zone for a PortShield interface that has different attributes to it than any of the default zones provide. To create a new zone for a PortShield interface, perform the following:

1. In the **Add PortShield Interface** window, click on the **Zone** list box and click on the **Create New Zone** option. The management software displays the General Settings dialog box.



2. Type a name in the **Name** field that will identify the new zone.
3. Click on the **Security Type** list box and click on a security type option that will classify the zone as having a certain level of access. The choices are:
  - **Trusted** - This security type offers the highest level of security, indicating that only trust, indicating that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the device. The LAN zone is always Trusted.
  - **Public** - This security type offers a higher level of security than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the device and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN.
  - **Wireless** - This security type applies to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. You typical use WiFiSec to secure traffic in a wireless zone.

- After selecting the security level for the PortShield interface, click on one of the following checkboxes that enables a security service for the zone:

Checkbox	Description
Allow Interface Trust	Automates the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance.
Enforce Content Filtering Service	Enforces protection and productivity policies for organizations to reduce legal and privacy risks while minimizing administration overhead.
Enforce Client Anti-Virus Service	Enables network-level inspection of email, Web traffic, file transfers, various stream-based protocols, instant messaging, and peer-to-peer applications to detect and clean malicious code, viruses, and worms.
Enable Gateway Anti-Virus Service	Enables gateway-level inspection of email, Web traffic, file transfers, various stream-based protocols, instant messaging, and peer-to-peer applications to detect and clean malicious code, viruses, and worms.
Enable IPS	Enables Intrusion Prevention Service which provides a configurable, high-performance deep packet inspection architecture using parallel searching algorithms through the application layer to deliver complete Web and E-Mail attack prevention.
Enable Anti-Spyware Service	Enables spyware protection which prevents malicious spyware from infecting networks by blocking related installations at the gateway and disrupting background communications from existing spyware programs.
Enforce Global Security Clients	Enables the application of the SonicWALL Global Security Client that delivers comprehensive desktop security for remote/mobile workers and corporate networks.
Create Group VPNs	Enables group VPN creation.

- Click **OK**.

## Refining the PortShield Interface

You can refine a PortShield interface group in the Switch Ports environment. To refine a PortShield interface group, perform the following steps:

- Log in to the security appliance.
- Click on the **Switch Ports** option. The following items are displayed:
  - A list of all interfaces including PortShield interfaces. Note the ports you have selected are parts of the PortShield interface you just created.
  - An interactive graphic of the ports on the switch



- If there are more ports you want to add to the PortShield interface, in the interactive switch ports graphic, select the ports you want to include in the PortShield interface group.

- Click the **Configure** button. The management software displays the Edit Multiple Switch Ports dialog box. You can refine your settings in this dialog box.



The name of the PortShield interface group will be assigned by default.

- Click on the **Port Enable** list box and click on either the **Enable** or **Disable** option to either activate or deactivate the interfaces in the PortShield interface group.
- Click on the **PortShield** interface list box and click on the PortShield interface you created in the previous procedure.
- Click on the **Link Speed** list box and click on a throughput speed you want to assign the interface. The choices are:
  - Auto negotiate
  - 100Mbps Full Duplex
  - 100 Mbps Half Duplex
  - 10 Mbps Full Duplex
  - 10 Mbps Half Duplex



**Note**

Do not change this setting from the default of Auto negotiate unless your system requires you to do so. Also, note that for any setting involving the Full Duplex feature to work properly, be sure to configure Full Duplex on both ends of the link. By not having Full Duplex configured on both ends, a duplex mismatch occurs, causing throughput loss.

- Click **OK**. Wait for a few seconds. The system then will incorporate the changes you made to the PortShield interface Group and add it back to the switch ports list.



## Creating Transparent Mode PortShield Interfaces

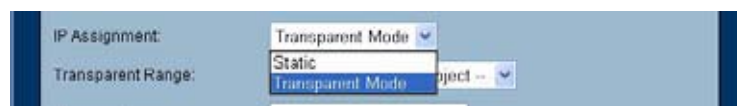
You may find it useful to create address objects to bundle addresses into address objects and reference these objects when creating a PortShield interface. Address objects allow for entities to be defined one time and to be reused in multiple referential instances throughout SonicOS. The PortShield interface creation environment provides a convenient way to reference address objects.

The following example takes a network with a series of addresses in the range 67.115.118.80/24 and divides it into three PortShield Interfaces, mapping each to the following ports and address objects:

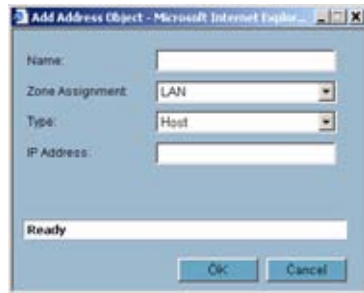
PortShield Interface	Port Numbers Mapped	Address Object Type	Address(es)
portshield1	5	Address Object Host	67.115.118.90/32
portshield2	6, 7, 8	Address Object Range	67.115.118.100-67.115.118.102
portshield3	2, 3	Address Object Host Group	67.115.118.200, 67.115.118.210, 67.115.118.212, 67.115.118.220, 67,115,118,230

To create these PortShield interfaces, using the prescribed address objects, perform the following steps:

1. Log in to the security appliance.
2. Navigate to **Network > Interfaces**. The Interfaces Settings page displays.
3. Click the **Add PortShield Interface** button. The management software displays the Add Port Shield dialog box.
4. Click the **Zone** list box and click on a zone type option to which you want to map the interface. For this exercise, click the LAN option. After you select a zone option, the management software displays a more expanded version of the PortShield Interface Settings dialog box. Only interfaces assigned to Trusted and Public zones can operate in Transparent mode.
5. Type a name in the **PortShield Interface Name** field.
6. Click on the **IP Assignment** list box and click the **Transparent Mode** option.



- Click on the **Transparent Range** list box and click on the **Create** new address object option. The management software displays the Add Address Object dialog box.



- Fill out the fields as detailed in the next three sections to create the three different types of address objects. The three examples use a subnetwork of 67.115.118.0.

## Creating a Transparent Mode PortShield Interface with a Host Address Object

To assign the Host Address Object 67.115.118.90 to portshield1, perform the following steps:

- Type the name **portshield1** in the **Name** field to identify the address object.
- Click the **Zone Assignment** list box and click the **LAN** option.
- Click the **Type** list box and click the **Host** option to make the address object apply to a single IP address. Note the Host option is the default option in the list box.
- Type your IP address, in this example, 67.115.118.90, in the **IP Address** field. The management software assumes a subnetwork mask of 255.255.255.255 (67.115.118.90/32). Note that because of this assumption, the software does not display a field for a subnetwork mask. Also, the field does not allow you to type enough a /32 notation as part of the address.
- Click **OK**. The General tab of the Port Shield dialog box is displayed.
- Click the **Switch Ports** tab. The Switch Ports tab is displayed.
- Click on **P5** in the Available Ports list and click the right arrow ( > ) button to move the port into the Assigned Ports list.
- Click **OK**. The Interfaces list displays, along with the new PortShield interface in the list. It displays the name, zone, IP address, subnetwork mask, IP assignment method, status, and comment, and link type status information about the address object you created (portshield1).



### Note

The IP address is the actual subnetwork address, not the specific address you entered. In this example, the address is 67.115.118.0 and not 67.115.118.90. This is because in Transparent mode, the interface appears to users as having the same address as the gateway. Therefore your explicit address is invisible or transparent to internet users. It lets you keep assigned IP addresses in the WAN subnet while protecting those hosts with full SonicWALL firewall protection (including services, etc.).

- Click on the **Switch Ports** option in the left navigation pane.
- In the graphic of the switch, view port number 5 and verify that the port is colored blue.
- In the switch port list, view the PortShield Interface column for P5 (port 5) and verify that the interface listed is portshield1.
- Refine the configuration of the PortShield Interface. For details, refer to the "Refining the PortShield Interface" on page 167.

## Creating a PortShield Using an Address Object Containing an Address Range

To assign a Range Address Object with addresses extending from 67.115.118.100 to 67.115.118.102 to portshield2, perform the following steps:

1. Type the name **portshield2** in the **Name** field to identify the address object.
2. Click the **Zone Assignment** list box and click the LAN option.
3. Click the **Type** list box and click the **Range** option to make the address object apply to a range of addresses. The management software displays new fields in the Add Address Object dialog box.



4. Note the Starting IP Address and Ending IP Address fields in the dialog box.
5. Type a starting IP address, in this example, 67.115.118.100, in the **Starting IP Address** field to establish this address as the minimum value in the range.
6. Type an ending IP address, in this example, 67.115.118.102, in the **Ending IP Address** field to establish this address as the maximum value in the range.
7. Click **OK**. The management software displays the General tab of the Port Shield dialog box.
8. Click the **Switch Ports** tab. The management software displays the Switch Ports tab.
9. Holding down the shift key, click on **P6**, **P7**, and **P8** in the **Available Ports** list and click the right arrow (>) button to move the port into the Assigned Ports list.
10. Click **OK**. Note it displays the name, zone, IP address, subnet mask, IP assignment method, status, comment, and link type status detail about the address object you created (portshield2).
11. Click on the **Switch Ports** option in the left navigation pane.
12. In the graphic of the switch, view port numbers 6, 7, and 8, and verify the port is colored blue.
13. In the switch port list, view the PortShield Interface column for P6, P7, and P8 and verify that the interface listed is portshield2.
14. Refine the configuration of the PortShield Interface. For details, refer to the "Refining the PortShield Interface" on page 167.

## Creating a Transparent Mode PortShield Interface with a Group Address Object

To assign a Group Address Object with addresses 67.115.118.200, 67.115.118.210, 67.115.118.212 67.115.118.220, and 67.115.118.230 to portshield3, perform the following steps:

1. To add a Group Address Object, navigate to **Networks > Address Objects**.

- Click on the **Add** button in the Address Objects list in the window. SonicOS displays the Add Address Object dialog box as shown in the following figure:



- Enter the name **portshield3** in the Name field.
- Select **Network** from the **Type** menu.
- Enter 67.115.118.200 in the network IP address and 255.255.255.0 in the **Netmask** field.
- Click on the **Zone Assignment** list box and click on **LAN**.
- Click **OK**. The Address Objects window displays the new portshield3 in the address group list.
- Repeat the procedure with the same settings for the following IP addresses: 67.115.118.210, 67.115.118.212, 67.115.118.220, and 67.115.118.230. Make sure the name of the address object for each address is portshield3. When you finish creating these address objects, you will only see portshield3 displayed in the address group list.
- Go back to the Add PortShield Interface dialog box and create an interface called portshield3 with a LAN zone, using a Transparent Mode address assignment type and select portshield3 from the Transparent Range list of existing address groups.
- Click on the **Switch Port** tab and add the ports 2 and 3 to the address object.
- Click **OK**. SonicOS displays the group address object portshield3 in the Interfaces list.
- Note the Network and Netmask fields in the dialog box.
- In the graphic of the switch, view port numbers 2 and 3, and verify that the port is colored blue.
- In the switch port list, view the PortShield Interface column for P2 and P3 (ports 2 and 3) and verify that the interface listed is portshield3.
- Refine the configuration of the PortShield Interface. For details, refer to the section, "Refining the PortShield Interface" on page 167.

## Mapping Ports from the Switch Ports Window

Another way to create a PortShield interface is to configure the interface in the Interfaces window and then assign ports to it in the Switch Ports window. Approaching it this way assumes you created a PortShield interface first and then selected the ports from the device ports graphic and selected the existing interface. This provides several advantages:

- Enables you to easily visualize the actual locations of ports.
- Separating the task of creating the interface, helps you focus more on how you want to separate the ports into different domains.

To select ports and apply them to a previously configured interface, perform the following steps:

1. Create a PortShield interface following the steps in “Overview” on page 160, but do not map ports to it by going into the Switch Ports tab.
2. Click the **Networks** option in the navigation pane and then click the **Switch Ports** option. SonicOS displays the Switch Ports window.
3. Note the color of the ports. While you can map any port, no matter what its color, to an interface, you should be aware of whether it has been selected for use in another PortShield interface.
  - From the device graphic, see if any of the ports you want to select appear in black or another color. If they are black, they are unused by another PortShield interface. If they are another color, they are in use. Just be cognizant of ones that are being used and what impact your remapping the port will have on the existing interface.
  - From the Switch Ports list, see if any of the ports in the PortShield Interface list have been selected as a PortShield interface.

Be cognizant of ones that are being used and what impact your remapping the port will have on the existing interface.

4. On the appliance graphic, click on ports 3, 4, and 5. The selected port graphics appear as yellow as shown in the following figure (if you are viewing this document in color).

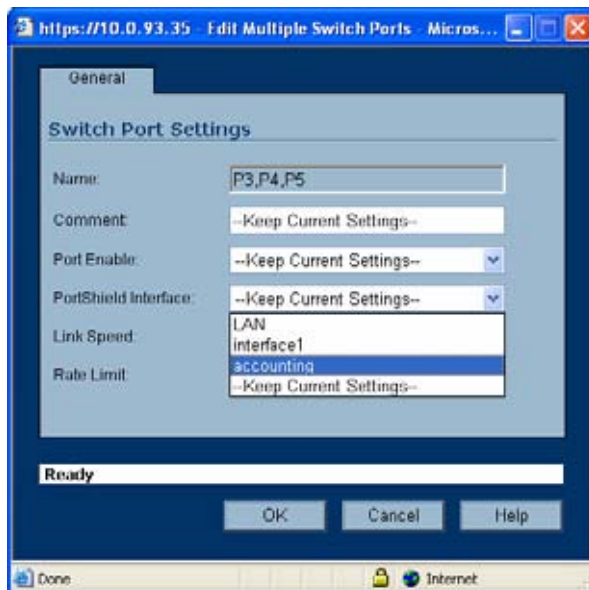


5. Click the **Configure** button. SonicOS displays the Switch Port Settings dialog box as shown in the following figure.



Note the Name field displays the ports you selected (P3, P4, P5).

- Click on the **PortShield Interface** list box as shown in the following figure.



Note the list contains the entry called **Accounting**. This is the host address object you created.

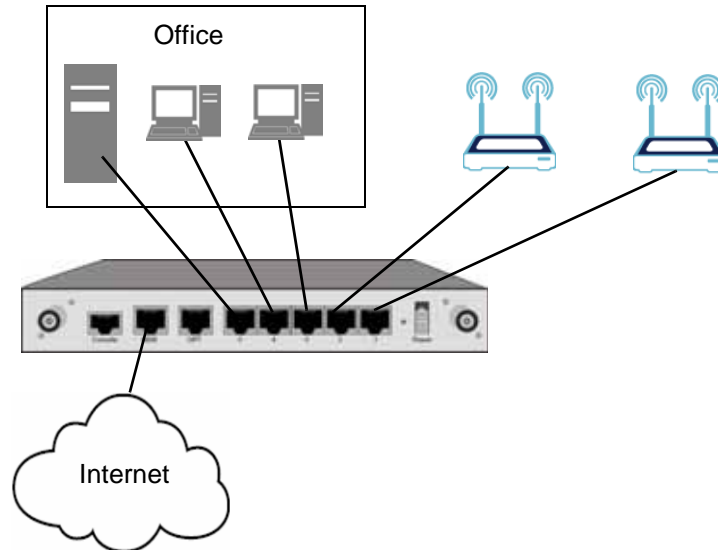
- Click on the **Accounting** entry. By selecting this entry, you mapped ports 3, 4, and 5 to the Accounting entry.
- Click **OK**. Wait a moment. SonicOS displays the Switch Ports dialog box, displaying the results of your session.
- Verify the PortShield interface port mappings.
  - In the device graphic, note SonicOS changed the color of ports 3, 4, and 5 from black to blue, indicating you successfully mapped them to a PortShield interface.
  - In the Switch Ports list, view the PortShield Interface column for ports 3, 4, and 5. This column now displays a blue-colored icon and the accounting string for P3, P4, and P5, indicating these ports are now mapped to the accounting PortShield interface.

## PortShield Deployment Scenario

A SonicWALL TZ 180 or TZ 190 with PortShield can be used in a small hotel or apartment setting. In this example, a SonicWALL TZ 180 with PortShield is used to provide access to an apartment complex. Two sonicpoints give wireless access to residents, and a small office LAN contains two computers and a mail and web server.

**Note**

The easiest way to configure this example is to use the PortShield Wizard. Configure it to have two PortShield interfaces, with three and two ports respectively. For more details on the PortShield Wizard, see **Chapter 23, Configuring PortShield Interfaces Using the Setup Wizard**.



## Deployment Details

This example uses the following zones and PortShield interfaces:

### Zones

- **LAN:** Default LAN zone configuration.
  - Used for Office PortShield Group.
  - All SonicWALL Security Services enabled.
- **Residents:** A custom zone for the General Users PortShield group. Residents is a Wireless zone with SonicPoint Enforcement disabled so it can be used like a LAN with mixed wired and wireless clients.
  - Used for the Residents PortShield group.
  - Zone Type: Wireless
  - All SonicWALL Security Services enabled.
  - **Only allow traffic generated by a SonicPoint** is not checked, disabling SonicPoint Enforcement. This setting allows the zone to be used for both wired and wireless traffic.
  - **Enable Wireless Guest Services** is checked. With SonicPoint enforcement disabled, this enables both wired and wireless guest services.
  - **Enable Dynamic Address Translation (DAT)** is checked. With SonicPoint enforcement disabled, this enables DAT for both wired and wireless guests.

## PortShield Interfaces

The small business example uses two PortShield interfaces.

- LAN: for office use
  - LAN zone
  - Ports 1 - 3. These ports are assigned to LAN by not assigning them to another PortShield interface.
  - 2 desktop workstations
  - 1 web and mail server.
  - No wireless access
- PortShield Interface 1
  - A Resident custom Wireless zones with SonicPoint enforcement disabled
  - Ports 3 and 4: one port for each PortShield interface
  - Two SonicPoints connected, covering the whole complex and providing seamless roaming.
  - Wireless Guest Services enabled

## Configuring the Hospitality Example Deployment

Configuring the hospitality example deployment involves the following procedures:

- “Configure the SonicPoint Profile” on page 176
- “Configure the Zones” on page 176
- “Configure the PortShield Interfaces with the PortShield Wizard” on page 179

### Configure the SonicPoint Profile

This example uses two SonicPoints to grant wireless access to users throughout the complex. Residents can log in with their accounts, and guest users can log in using Wireless Guest Services. The SonicPoint profile contains the settings that the security appliance automatically applies to all connected SonicPoints.

Follow the procedures in [“SonicPoint > SonicPoints” section on page 391](#) and configure the SonicPoint profile. Keep the defaults except where appropriate for your installation. Set the SSID for both 802.11a and 802.11g radios to a name that identifies the apartment complex or hotel, for example, “SonicWALL Arms Resident Internet.”

### Configure the Zones

This example uses two zones inside its network, LAN and a custom zone, Residents. Residents is a Wireless zone with SonicPoint Enforcement disabled, thus allowing both wireless and wired access. Guest services is enabled, allowing both wired and wireless guest users access to the internet.

For more details on configuring zones, see [Chapter 17, Configuring Zones](#).

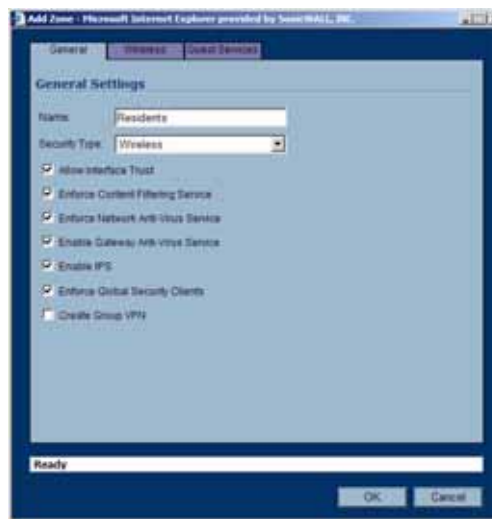
**LAN:** Leave the default configuration for these two zones.

**Residents:** Configure the Residents zone with the following values:

- **General** tab settings:



- **Name:** Residents
- **Security Type:** Wireless. Select Wireless so you can use the same context for the both the individual wired connections and the SonicPoints.
- **Allow Interface Trust:** Checked
- **Enforce Content Filtering Service:** Checked
- **Enforce Client Anti-Virus Service:** Checked
- **Enable Gateway Anti-Virus Service:** Checked
- **Enable IPS:** Checked
- **Enforce Global Security Clients:** Only check if you want to require SonicWALL Global Security Client for your residents to log into the network
- **Create Group VPN:** Only Check if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.



- **Wireless** tab settings:
  - **Only allow traffic generated by a SonicPoint:** Leave this option unchecked. This disables SonicPoint enforcement, allowing both wired and wireless connections through this zone.
  - **SSL-VPN Enforcement:** Only check this option if you want to enforce SSL-VPN security, requiring your residents to use an SSL-VPN client to connect.
  - **WiFiSec Enforcement:** Only check this option if you want to enforce WiFiSec security, requiring your residents to use a VPN client to connect.

- **SonicPoint Provisioning Profile:** Select the SonicPoint profile you configured. The settings in this profile will automatically be applied to the SonicPoints you set up for wireless access.



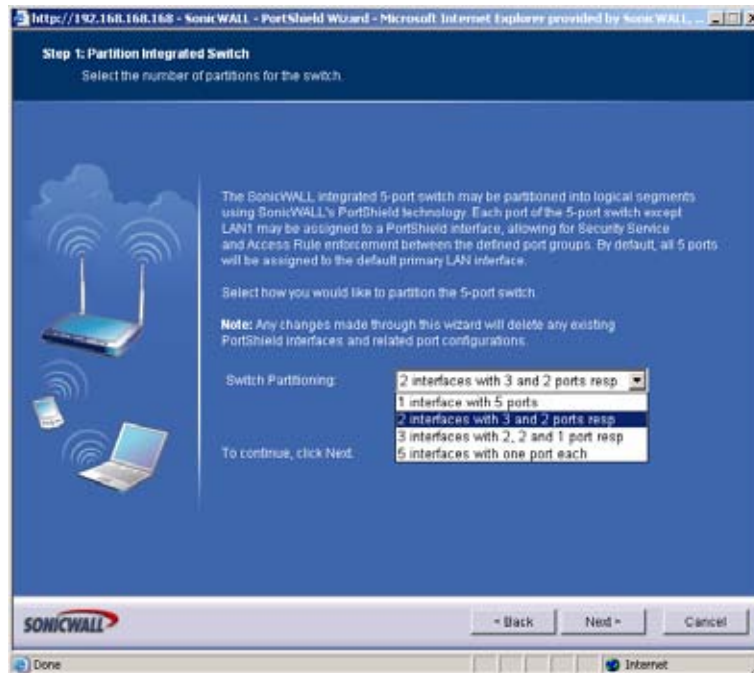
- **Guest Services** tab settings:
  - **Enable Wireless Guest Services:** Check this option to enable access to the internet for guest users who do not have resident accounts.
  - **Enable Dynamic Address Translation (DAT):** Check this option to enable guest users to connect without having to change their internet connection settings. See [Chapter 17, Configuring Zones](#) for more information on DAT.
  - **Custom Authentication Page:** Only check this option if you want to create a custom login page for guest users.



## Configure the PortShield Interfaces with the PortShield Wizard

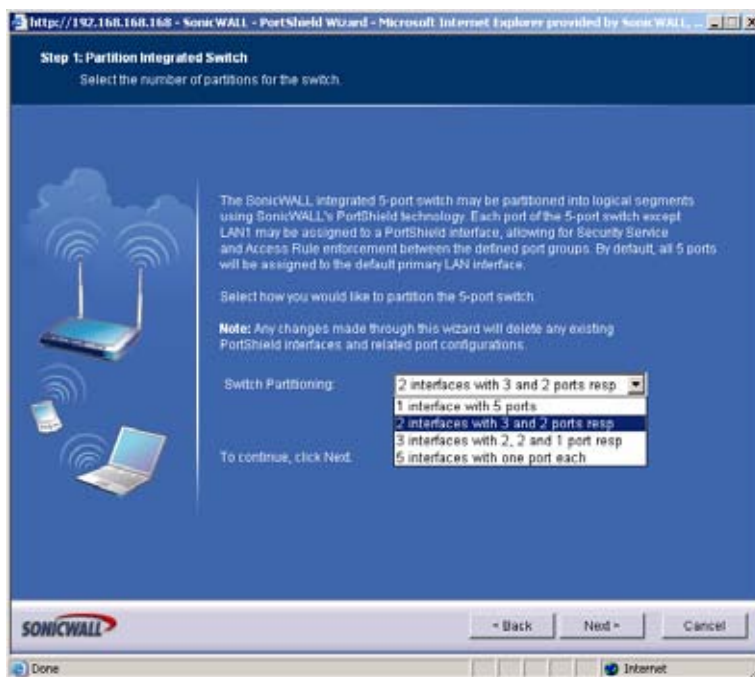
In this example, two ports are assigned to a Wireless PortShield interface for the SonicPoints and three ports are assigned to the LAN interface for the Office. The easiest way to configure this is to use the PortShield Wizard and then modify the configuration. We will use the wizard to configure 2 PortShield interfaces with 3 and 2 ports respectively.

1. On the **Network > SwitchPorts** page, click the **PortShield Wizard** button to launch the PortShield Wizard. click **Next**.
2. Select **2 PortShield interfaces with 3 and 2 ports resp** and click **Next**.



3. Select **Auto-configure PortShield interfaces** to have the wizard assign an IP address to PortShield Interface 1. Select **Configure PortShield interfaces manually** if you want to specify the IP address yourself.

- Uncheck the **Enable Interface Trust for new PortShield Interface segments** checkbox to prevent communication between the wireless segment and the office segment. If this level of security is not necessary, leave the checkbox checked. You can modify these settings on the **Firewall > Access Rules** page. Click **Next**.



- Click **Apply** to create the interfaces.

The SonicWALL TZ 180 is now configured such that ports 1, 2, and 5 are for the office LAN, and ports 3 and 4 are for wireless access.



## CHAPTER 16

# Setting Up WAN Failover and Load Balancing

---

## Network > WAN Failover & Load Balancing

WAN Failover and Load Balancing allows you to designate the one of the user-assigned interfaces as a Secondary or backup WAN port. The secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through the secondary WAN port if the primary WAN port is down and/or unavailable. In this chapter, this feature is referred to as *basic failover*. This allows the SonicWALL security appliance to maintain a persistent connection for WAN port traffic by failing over to the secondary WAN port. The primary and secondary WAN ports can also be used in a more dynamic active/active setup, where the administrator can choose a method of dividing outbound traffic flows between the Primary fixed WAN port and the user-assigned Secondary WAN port. This latter feature is referred to as *load balancing*.

### WAN Failover Caveats

- WAN Failover and Load Balancing applies to outbound-initiated traffic only; it cannot be used to perform inbound Load Balancing functions, such as what a content switching or Load Balancing appliance provides.
- Make sure that the SonicWALL security appliance has the proper NAT policies for the Secondary WAN interface an incorrect or missing NAT Policy for the Secondary WAN port is the most common problem seen when configuring WAN Failover & Load Balancing.
- The Primary and Secondary WAN ports cannot be on the same IP subnet; each WAN connection must be on unique IP subnets in order to work properly
- You cannot use the WAN failover feature if you have configured the SonicWALL security appliance to use Transparent Mode in the **Network > Interfaces** page.

## About Source and Destination IP Address Binding

When you establish a connection with a WAN, you can create multiple interfaces, dividing up the task load over these interfaces. There are both Primary and Secondary WAN interfaces. This task distribution model maintains high performance, ensuring that one interface does not become an impasse to the point where it blocks traffic from passing. This process is WAN Load Balancing.

While WAN Load Balancing addresses performance challenges, it can create other problems, including losing track of sessions. Session confusion can occur because some applications fail to adequately track multiple user sessions Load Balanced on multiple interfaces. These applications treat incoming packets as originating from different users because they use IP addresses to differentiate user sessions instead of application-layer user identification tags.

To ensure that you have proper connectivity in all applications, SonicWALL provides a feature called Source and Destination IP Addresses Binding, a solution that maintains a consistent mapping of traffic flows with a single outbound WAN interface.

## Setting Up WAN Failover and Load Balancing

Perform the following steps to configure WAN Failover and Load Balancing on the SonicWALL security appliance:

1. [“Configuring an Interface as a Secondary WAN Port” on page 182](#)
2. [“Creating a NAT Policy for the Secondary WAN Port” on page 183](#)
3. [“Activating WAN Failover and Selecting the Load Balancing Method” on page 184](#)
4. [“Configuring WAN Interface Monitoring” on page 186](#)
5. [“Configuring WAN Probe Monitoring” on page 187](#)

## Configuring an Interface as a Secondary WAN Port

On **Network > Interfaces** page, configure the chosen port to be in WAN zone, and enter in the correct address settings provided by the Secondary ISP. In the example, the SonicWALL security appliance is acquiring its secondary WAN address dynamically from ISP #2, using DHCP. Any interface added to the WAN zone by default creates a NAT Policy allowing internal LAN subnets to NAT out this Secondary WAN interface.

## Creating a NAT Policy for the Secondary WAN Port

You need to create a NAT policy on your SonicWALL for WAN Failover. Follow these steps to create a NAT policy on your SonicWALL using the **OPT** interface:

- 
- Step 1** Select **Network > NAT Policies**.
  - Step 2** Click **Add**. The **Add NAT Policy** window is displayed.
  - Step 3** Select **Any** from the **Original Source** menu.
  - Step 4** Select **OPT IP** from the **Translated Source** menu.
  - Step 5** Select **Any** from the **Original Destination** menu.
  - Step 6** Select **Original** from the **Translated Destination** menu.
  - Step 7** Select **Any** from the **Original Service** menu.
  - Step 8** Select **Original** from the **Translated Service** menu.
  - Step 9** Select **LAN** from the **Inbound Interface** menu.
  - Step 10** Select **OPT** interface from the **Outbound Interface** menu.
  - Step 11** Make sure the **Enable** setting is checked.
  - Step 12** Click **OK**.

## Activating WAN Failover and Selecting the Load Balancing Method

To configure the SonicWALL for WAN failover and load balancing, follow the steps below:

- Step 1** On **Network > WAN Failover & LB** page, select **Enable Load Balancing**.

**Network > WAN Failover & Load Balancing** Clear Statistics Apply Cancel ?

**Ethernet WAN Failover & Load Balancing**

Primary WAN Interface:

Secondary WAN Interface:

Enable Load Balancing

Basic Active/Passive Failover

Preempt and fallback to Primary WAN when possible

Per Connection Round-Robin

Spillover-Based

Send traffic to Secondary WAN when bandwidth exceeds  Kbps

Percentage-Based

Use Source and Destination IP Addresses Binding

Primary WAN Percentage:

Secondary WAN Percentage:

**WAN Load Balancing Statistics**

WAN interface Statistics	WAN	Modem
Link Status:	Link Up	Link Down
Load Balancing State:	Active - Available	Admin Down
Probe Main Target:	Disabled	Disabled
Probe Alternate Target:	Disabled	Disabled
New Connections:	0	0
Total Connections:	0	0
Rx Unicast Packets:	3421581	0
Rx Bytes:	365606943	0
Tx Unicast Packets:	3557	0
Tx Bytes:	2241910	0
Tx Current Percentage:	100	0
Tx Current Throughput (KB/s):	1	0

**Dial-Up WAN Failover**

Enable Dial-Up Wan Failover

**Note:** Dial-Up is used when no WAN Zone Ethernet connection is available.

**WAN Interfaces Monitoring**

Check interface every  seconds

Deactivate interface after  missed intervals

Reactivate interface after  successful intervals

Enable Probe Monitoring Configure

Respond to Probes

Any TCP-SYN to Port

- Step 2** If there are multiple possible secondary WAN interfaces, select an interface from the **Secondary WAN Interface**.

- Step 3** Select a load balancing method. By default, the SonicWALL will select **Basic Active/Passive Failover** as the method, but there are four load balancing methods available:



**Ethernet WAN Failover & Load Balancing**

Primary WAN Interface:

Secondary WAN Interface:

Enable Load Balancing

Basic Active/Passive Failover

Preempt and failback to Primary WAN when possible

Per Connection Round-Robin

Spillover-Based

Send traffic to Secondary WAN when bandwidth exceeds:  Kbps

Percentage-Based

Use Source and Destination IP Addresses Binding

Primary WAN Percentage:

Secondary WAN Percentage:

- **Basic Active/Passive Failover:** When this setting is selected, the SonicWALL security appliance only sends traffic through the Secondary WAN interface if the Primary WAN interface has been marked inactive. The SonicWALL security appliance is set to use this as the default load balancing method. If the Primary WAN fails, then the SonicWALL security appliance reverts to this method instead of the ones described below. This mode will automatically return back to using the Primary WAN interface once it has been restored (preempt mode).

This item has an associated **Preempt and fail back to Primary WAN when possible** checkbox. When this checkbox is selected, the SonicWALL security appliance switches back to sending its traffic across the Primary WAN interface when it resumes responding to the SonicWALL security appliance's checks (the WAN's physical link is restored, or the logical probe targets on the WAN port resume responding).

- **Per Destination Round-Robin:** When this setting is selected, the SonicWALL security appliance Load Balances outgoing traffic on a per-destination basis. This is a simple load balancing method and, though not very granular, allows you to utilize both links in a basic fashion (instead of the method above, which does not utilize the capability of the Secondary WAN until the Primary WAN has failed). The SonicWALL security appliance needs to examine outbound flows for uniqueness in source IP and destination IP and make the determination as to which interface to send the traffic out of and accept it back on. Please note this feature will be overridden by specific static route entries.
- **Spillover-Based:** When this settings is selected, the user can specify when the SonicWALL security appliance starts sending traffic through the Secondary WAN interface. This method allows you to control when and if the Secondary interface is used. This method is used if you do not want outbound traffic sent across the Secondary WAN unless the Primary WAN is overloaded.

Specify the maximum allowed bandwidth on the primary WAN interface in the **Send traffic to Secondary WAN interface when bandwidth exceeds \_ Kbps** field. The SonicWALL security appliance has a non-Management Interface exposed hold timer set to 20 seconds – if the sustained outbound traffic across the Primary WAN interface exceeds the administrator defined bps, then the SonicWALL security appliance spills outbound traffic to the Secondary WAN interface (on a per-destination basis). Please note this feature will be overridden by specific static route entries.

- **Percentage-Based:** When this setting is selected, you can specify the percentages of traffic sent through the Primary WAN and Secondary WAN interfaces. This method allows you to actively utilize both Primary and Secondary WAN interfaces. Only one

entry box is required (percentage for Primary WAN) The management interface automatically populates the non-user-editable entry box with the remaining percentage assigned to the Secondary WAN interface. Please note this feature will be overridden by specific static route entries.

- **Use Source and Destination IP Address Binding:** When you are using percentage-based load balancing, this checkbox enables you to maintain a consistent mapping of traffic flows with a single outbound WAN interface, regardless of the percentage of traffic through that interface. Therefore, the outbound IP address of the connection remains consistent. However the percentage of traffic in each WAN interface may not match the percentage you specify in the **Primary WAN Percentage** field.

This method uses only the source IP address and the destination IP address to determine when to bind a connection to a single interface and ignores all other information, such as source and destination TCP port numbers.

**Step 4** Click **Apply**.

## Configuring WAN Interface Monitoring



Under the **WAN Interface Monitoring** heading, you can customize how the SonicWALL security appliance monitors the WAN interface:

- Enter a number between 5 and 300, in the **Check Interface Every \_ Seconds** field. The default value is 5 seconds.
- In the **Deactivate Interface after \_ missed intervals**, enter a number between 1 and 10. The default value is 3, which means the interface is considered inactive after 3 consecutive unsuccessful attempts.
- Enter a number between 1 and 10 in the **Reactivate Interface after \_ successful intervals**. The default value is 3, which means the interface is considered active after 3 consecutive successful attempts.

## WAN Probe Monitoring

If Probe Monitoring is not activated, the SonicWALL security appliance performs physical monitoring only on the Primary and Secondary WAN interfaces, meaning it only marks a WAN interface as failed if the interface is disconnected or stops receiving an Ethernet-layer signal. This is not an assured means of link monitoring, because it does not address most failure scenarios (for example, routing issues with your ISP or an upstream router that is no longer passing traffic). If the WAN interface is connected to a hub or switch, and the router providing the connection to the ISP (also connected to this hub or switch) were to fail, the SonicWALL will continue to believe the WAN link is usable, because the connection to the hub or switch is good.

Enabling probe monitoring on the **Network > WAN Failover & Load Balancing** page instructs the SonicWALL security appliance to perform logical checks of upstream targets to ensure that the line is indeed usable, eliminating this potential problem, as well as continue to do physical monitoring. Under the default probe monitoring configuration, the SonicWALL performs an ICMP ping probe of both WAN ports' default gateways. Unfortunately, this is also not an assured means of link monitoring, because service interruption may be occurring farther

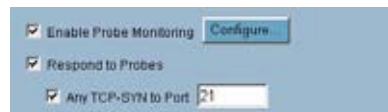
upstream. If your ISP is experiencing problems in its routing infrastructure, a successful ICMP ping of their router causes the SonicWALL security appliance to believe the line is usable, when in fact it may not be able to pass traffic to and from the public Internet at all.

To perform reliable link monitoring, you can choose ICMP or TCP as monitoring method, and can specify up to two targets for each WAN port. TCP is preferred because many devices on the public Internet now actively drop or block ICMP requests. If you specify two targets for each WAN interface, you can logically link the two probe targets such that if either one fails the line will go down, or that both must fail for the line to be considered down. Using the latter method, you can configure a sort of 'deep check' to see if the line is truly usable – for instance, you could set first probe target of your ISP's router interface using ICMP (assuming they allow this), and then do a secondary probe target of a DNS server on the public Internet using TCP Port 53. With this method, if the ICMP probe of the ISP's router fails but the farther upstream continues to respond, the SonicWALL security appliance assumes the link is usable and continue to send traffic across it.

## Configuring WAN Probe Monitoring

To configure WAN probe monitoring, follow these steps:

- Step 1** On the **Network > WAN Failover & Load Balancing** page, under the **WAN Interface Monitoring** heading, check the **Enable Probe Monitoring** box.



- Step 2** Check the **Respond to Probes** box to have the SonicWALL security appliance respond to SonicWALL TCP probes received on any of its WAN ports. Do not check this box if the SonicWALL security appliance should not respond to TCP probes.
- Step 3** Check the **Any TCP-SYN to Port** box to instruct the SonicWALL security appliance to respond to TCP probes to the specified port number without validating them first. The **Any TCP-SYN to Port** box should only be checked when receiving TCP probes from SonicWALL security appliances running SonicOS Standard or older, legacy SonicWALL security appliances.



**Note**

If there is a NAT device between the two devices sending and receiving TCP probes, the **Any TCP-SYN to Port** box must be checked, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.

**Step 4** Click on the **Configure** button. The **Configure WAN Probe Monitoring** window is displayed.



**Step 5** In the **Primary WAN Probe Settings** menu, select one of the following options:

- Probe succeeds when either Main Target or Alternate Target responds
- Probe succeeds when both Main Target and Alternative Target respond
- Probe succeeds when Main Target responds
- Succeeds Always (no probing)

**Step 6** Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.

**Step 7** Enter the IP address of the target device in the **IP Address** field.

**Step 8** Enter a port number in the **Port** field.

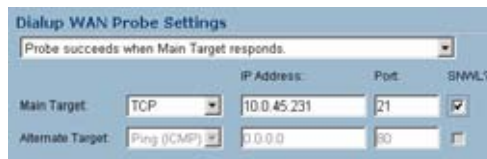


**Note**

If there is a NAT device between the two devices sending and receiving TCP probes, the **Any TCP-SYN to Port** box must be checked, and the same port number must be configured here and in the **Configure WAN Probe Monitoring** window.

**Step 9** Check the **SNWL?** box if the target device is a SonicWALL security appliance. Do not check the **SNWL?** box for third-party devices, as the TCP probes may not work consistently.

**Step 10** Configure the **Secondary WAN Probe Settings**, which provide the same options as the **Primary WAN Probe Settings**.



**Step 11** Click **OK**.

**Caution** Before you begin, be sure you have configured a user-defined interface to mirror the WAN port settings.



**Note** If the Probe Target is unable to contact the target device, the interface is deactivated and traffic is no longer sent to the primary WAN.

## WAN Load Balancing Statistics

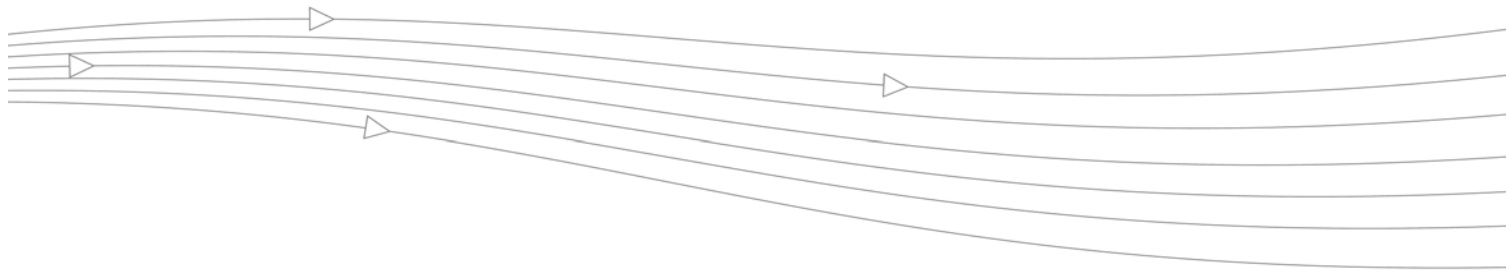
The **WAN Load Balancing Statistics** table displays the following WAN Interface statistics for the SonicWALL:

WAN Load Balancing Statistics		
WAN Interface Statistics	X1	X4
Link Status:	Link Up	Link Down
Load Balancing State:	Active - Available	Failover
Probe Main Target:	No probing	No probing
Probe Alternate Target:	No probing	No probing
New Connections:	1539	0
Total Connections:	40356	0
Rx Unicast Packets:	17912	0
Rx Bytes:	112520961	0
Tx Unicast Packets:	21080	0
Tx Bytes:	11177641	0
Tx Current Percentage:	0	0
Tx Current Throughput (KB/s):	31	0

- Link Status
- Load Balancing State
- Probe Monitoring
- New Connections
- Total Connections
- Rx Unicast Packets
- Rx Bytes
- Tx Unicast Packets
- Tx Bytes
- Tx Current Percentage
- Tx Current Throughput (KB/s)

Click the **Clear Statistic** button on the top right of the **Network > WAN Failover & Load Balancing** page to clear information from the **WAN Load Balancing Statistics** table.





# CHAPTER 17

## Configuring Zones

---

### Network > Zones

A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules, a simpler and more intuitive process than following strict physical interface scheme. Zone-based security is a powerful and flexible method of managing both internal and external network segments, allowing the administrator to separate and protect critical internal network resources from unapproved access or attack.

A network security zone is simply a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. Security zones provide an additional, more flexible, layer of security for the firewall. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface.

For more information on configuring interfaces, see the [“Network > Interfaces” section on page 137](#).

SonicOS Enhanced zones allows you to apply security policies to the inside of the network. This allows the administrator to do this by organizing network resources to different zones, and allowing or restricting traffic between those zones. This way, access to critical internal resources such as payroll servers or engineering code servers can be strictly controlled.

Zones also allow full exposure of the NAT table to allow the administrator control over the traffic across the interfaces by controlling the source and destination addresses as traffic crosses from one zone to another. This means that NAT can be applied internally, or across VPN

tunnels, which is a feature that users have long requested. SonicWALL security appliances can also drive VPN traffic through the NAT policy and zone policy, since VPNs are now logically grouped into their own VPN zone.

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
LAN	Trusted	X0	✓			✓	✓	✓		[Icons]
WAN	Untrusted	X1				✓	✓	✓		[Icons]
DMZ	Public	X2	✓	✓						[Icons]
VPN	Encrypted	N/A								[Icons]
MULTICAST	Untrusted	N/A								[Icons]
WLAN	Wireless	N/A								[Icons]

## How Zones Work

An easy way to visualize how security zones work is to imagine a large new building, with several rooms inside the building, and a group of new employees that do not know their way around the building. This building has one or more exits, which can be thought of as the WAN interfaces. The rooms within the building have one or more doors, which can be thought of as interfaces. These rooms can be thought of as zones inside each room are a number of people. The people are categorized and assigned to separate rooms within the building. People in each room going to another room or leaving the building, must talk to a doorman on the way out of each room. This doorman is the inter-zone/intra-zone security policy, and the doorman's job to consult a list and make sure that the person is allowed to go to the other room, or to leave the building. If the person is allowed (i.e. the security policy lets them), they can leave the room via the door (the interface).

Upon entering the hallway, the person needs to consult with the hallway monitor to find out where the room is, or where the door out of the building is located. This hallway monitor provides the routing process because the monitor knows where all the rooms are located, and how to get in and out of the building. The monitor also knows the addresses of any of the remote offices, which can be considered the VPNs. If the building has more than one entrance/exit (WAN interfaces), the hallway monitor can direct people to use the secondary entrance/exit, depending upon how they've been told to do so (i.e. only in an emergency, or to distribute the traffic in and out of the entrance/exits). This function can be thought of as WAN Load Balancing.

There are times that the rooms inside the building have more than one door, and times when there are groups of people in the room who are not familiar with one another. In this example, one group of people uses only one door, and another group uses the other door, even though groups are all in the same room. Because they also don't recognize each other, in order to speak with someone in another group, the users must ask the doorman (the security policy) to point out which person in the other group is the one with whom they wish to speak. The doorman has the option to not let one group of people talk to the other groups in the room. This is an example of when zones have more than one interface bound to them, and when intra-zone traffic is not allowed.

Sometimes, people will wish to visit remote offices, and people may arrive from remote offices to visit people in specific rooms in the building. These are the VPN tunnels. The hallway and doorway monitors check to see if this is allowed or not, and allow traffic through. The doorman can also elect to force people to put on a costume before traveling to another room, or to exit, or to another remote office. This hides the true identity of the person, masquerading the person as someone else. This process can be thought of as the NAT policy.



## Predefined Zones

The predefined zones on your the SonicWALL security appliance depend on the device. The following are all the SonicWALL security appliance's predefined security zones:

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	Anti-Spyware	IPS	CSC	Configure
LAN	Trusted	X0	✓			✓	✓	✓		
WAN	Untrusted	X1				✓	✓	✓		
DMZ	Public	X2	✓	✓						
VPN	Encrypted	N/A								
MULTICAST	Untrusted	N/A								
WLAN	Wireless	N/A								

The predefined security zones on the SonicWALL security appliance are not modifiable and are defined as follows:

- **WAN:** This zone can consist of either one or two interfaces. If you're using the security appliance's WAN failover capability, you need to add the second Internet interface to the WAN zone.
- **LAN:** This zone can consist of one to five interfaces, depending on your network design. Even though each interface will have a different network subnet attached to it, when grouped together they can be managed as a single entity.
- **DMZ:** This zone is normally used for publicly accessible servers. This zone can consist of one to four interfaces, depending on you network design.
- **VPN:** This virtual zone is used for simplifying secure, remote connectivity. It is the only zone that does not have an assigned physical interface.
- **MULTICAST:** This zone provides support for IP multicasting, which is a method for sending IN packets from a single source simultaneously to multiple hosts.
- **WLAN:** This zone provides support to SonicWALL SonicPoints. When assigned to the Opt port, it enforces SonicPoint Enforcement, automatically dropping all packets received from non-SonicPoint devices. The WLAN zone supports SonicPoint Discovery Protocol (SDP) to automatically poll for and identify attached SonicPoints. It also supports SonicWALL Simple Provisioning Protocol to configure SonicPoints using profiles.



**Note**

Even though you may group interfaces together into one security zone, this does not preclude you from addressing a single interface within the Zone.

## Security Types

Each zone has a security type, which defines the level of trust given to that zone. There are five security types:

- **Trusted:** Trusted is a security type that provides the highest level of trust—meaning that the least amount of scrutiny is applied to traffic coming from trusted zones. Trusted security can be thought of as being on the LAN (protected) side of the security appliance. The LAN zone is always Trusted.
- **Encrypted:** Encrypted is a security type used exclusively by the VPN Zone. All traffic to and from an Encrypted zone is encrypted.
- **Wireless:** Wireless is a security type applied to the WLAN zone or any zone where the only interface to the network consists of SonicWALL SonicPoint devices. You typically use WiFiSec to secure traffic in a Wireless zone. The Wireless security type is designed specifically for use with SonicPoint devices. Placing an interface in a Wireless Zone activates SDP (SonicWALL Discovery Protocol) and SSPP (SonicWALL Simple Provisioning Protocol) on that interface for automatic discovery and provisioning of SonicPoint devices. Only traffic that passes through a SonicPoint is allowed through a Wireless zone; all other traffic is dropped.
- **Public:** A Public security type offers a higher level of trust than an Untrusted zone, but a lower level of trust than a Trusted zone. Public zones can be thought of as being a secure area between the LAN (protected) side of the security appliance and the WAN (unprotected) side. The DMZ, for example, is a Public zone because traffic flows from it to both the LAN and the WAN. By default traffic from DMZ to LAN is denied. But traffic from LAN to ANY is allowed. This means only LAN initiated connections will have traffic between DMZ and LAN. The DMZ will only have default access to the WAN, not the LAN.
- **Untrusted:** The Untrusted security type represents the lowest level of trust. It is used by both the WAN and the virtual Multicast zone. An Untrusted zone can be thought of as being on the WAN (unprotected) side of the security appliance. By default, traffic from Untrusted zones is not permitted to enter any other zone type without explicit rules, but traffic from every other zone type is permitted to Untrusted zones.

## Allow Interface Trust

The **Allow Interface Trust** setting in the **Add Zone** window automates the creation of Access Rules to allow traffic to flow between the interface of a zone instance. For example, if the LAN Zone has both the **LAN** and **OPT** interfaces assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.

## Enabling SonicWALL Security Services on Zones

You can enable SonicWALL Security Services for traffic across zones. For example, you can enable SonicWALL Intrusion Prevention Service for incoming and outgoing traffic on the WLAN zone to add more security for internal network traffic. You can enable the following SonicWALL Security Services on zones:

- **Enforce Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
- **Enforce Client Anti-Virus Service** - Enforces anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Gateway Anti-Virus** - Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable IPS** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.


- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enforce Global Security Clients** - Enforces security policies for Global Security Clients on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - Creates a GroupVPN policy for the Zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck **Create Group VPN**, the GroupVPN policy is removed from the **VPN > Settings** page.

## The Zone Settings Table

The **Zone Settings** table displays a listing of all the SonicWALL security appliance default predefined zones as well as any zones you create. The table displays the following status information about each zone configuration:

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Network AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
LAN	Trusted	X0	✓			✓	✓	✓		
WAN	Untrusted	X1				✓	✓	✓		
DMZ	Public	X2	✓	✓						
VPN	Encrypted	N/A								
MULTICAST	Untrusted	N/A								
WLAN	Wireless	N/A								

- **Name:** Lists the name of the zone. The predefined **LAN**, **WAN**, **WLAN**, **VPN**, and **Encrypted** zone names cannot be changed.
- **Security Type:** Displays the security type: **Trusted**, **Untrusted**, **Public**, **Wireless**, or **Encrypted**.
- **Member Interfaces:** Displays the interfaces that are members of the zone. VLAN sub-interfaces are denoted by the name of the physical interface and the VLAN tag number, for example: "X3:V100".
- **Interface Trust:** A check mark indicates the **Allow Interface Trust** setting is enabled for the zone.
- **Content Filtering:** A check mark indicates SonicWALL Content Filtering Service is enabled for traffic coming in and going out of the zone.
- **Client Anti-Virus:** A check mark indicates SonicWALL Client Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWALL Client Anti-Virus manages an anti-virus client application on all clients on the zone.
- **Gateway Anti-Virus:** A check mark indicates SonicWALL Gateway Anti-Virus is enabled for traffic coming in and going out of the zone. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
- **Anti-Spyware Service** - A check mark indicates SonicWALL Anti-Spyware detection and prevention is enabled for traffic through interfaces in the zone.
- **IPS:** A check mark indicates SonicWALL Intrusion Prevention Service is enabled for traffic coming in and going out of the zone.
- **GSC:** A check mark indicates SonicWALL Global Security Client is enabled for clients connecting to the zone.

- **Configure:** Clicking the Notepad icon  displays the Edit Zone window. Clicking the Trashcan icon  deletes the zone. The Trashcan icon is dimmed for the predefined zones. You cannot delete these zones.

## Adding a New Zone



To add a new Zone, click **Add** under the **Zone Settings** table. The **Add Zone** window is displayed.

- 
- Step 1** Type a name for the new zone in the **Name** field.
  - Step 2** Select a security type **Trusted**, **Public** or **Wireless** from the **Security Type** menu. Use **Trusted** for Zones that you want to assign the highest level of trust, such as internal LAN segments. Use **Public** for Zones with a lower level of trust requirements, such as a DMZ interface. Use **Wireless** for the WLAN interface.
  - Step 3** If you want to allow intra-zone communications, select **Allow Interface Trust**. If not, select the **Allow Interface Trust** checkbox.
  - Step 4** Select any of the SonicWALL Security Services you want to enforce on the zone. You can select:
    - **SonicWALL Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones. To apply a Content Filtering Service (CFS) policy to the zone, select the policy from the **CFS Policy** pull-down menu.
    - **SonicWALL Enforce Client Anti-Virus Service** - Enforces Client Anti-Virus protection on multiple interfaces in the same Trusted, Public or WLAN zones, using the SonicWALL Client Anti-Virus client on your network hosts.

- **Enable Gateway Anti-Virus Service** - Enforces gateway anti-virus protection on your SonicWALL security appliance for all clients connecting to this zone. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
- **SonicWALL Intrusion Protection Service (IPS)** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Enforce Global Security Clients** - Requires clients to use the SonicWALL Global Security Client (GSC) to secure their local machine. Causes GSC settings to be pushed from the security appliance to the network hosts.
- **Create Group VPN** - Automatically creates a SonicWALL GroupVPN Policy for this zone. You can customize the GroupVPN Policy in the **VPN > Settings** page.


---

**Caution** Unsetting the **Create Group VPN** checkbox will remove any corresponding GroupVPN policy.


---

**Step 5** Click **OK**. The new zone is now added to the SonicWALL security appliance.

## Deleting a Zone

You can delete a user-created zone by clicking the Trashcan icon  in the **Configure** column. The Trashcan icon is unavailable for the predefined Zones (LAN, WAN, DMZ, VPN, WLAN, and MULTICAST). You cannot delete these zones. Any zones that you create can be deleted.

## Configuring the WLAN Zone

- 
- Step 1** Click the Edit icon  for the WLAN zone. The **Edit Zone** window is displayed.
- Step 2** In the **General** tab, select the **Allow Interface Trust** setting to automate the creation of Access Rules to allow traffic to flow between the interfaces of a zone instance. For example, if the LAN Zone has both the **LAN** and **OPT** interfaces assigned to it, checking **Allow Interface Trust** on the LAN Zone creates the necessary Access Rules to allow hosts on these interfaces to communicate with each other.
- Step 3** Select any of the following settings to enable the SonicWALL Security Services on the WLAN zone:
- **Enforce Content Filtering Service** - Enforces content filtering on multiple interfaces in the same Trusted, Public and WLAN zones.
  - **Enforce Client Anti-Virus Service** - Enforces managed anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. SonicWALL Client Anti-Virus manages an anti-virus client application on all clients on the zone.
  - **Enable Gateway Anti-Virus** - Enforces gateway anti-virus protection on multiple interfaces in the same Trusted, Public or WLAN zones. SonicWALL Gateway Anti-Virus manages the anti-virus service on the SonicWALL appliance.
  - **Enable IPS** - Enforces intrusion detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.
  - **Enable Anti-Spyware Service** - Enforces anti-spyware detection and prevention on multiple interfaces in the same Trusted, Public or WLAN zones.

- **Enforce Global Security Clients** - Enforces security policies for Global Security Clients on multiple interfaces in the same Trusted, Public or WLAN zones.
- **Create Group VPN** - creates a GroupVPN policy for the Zone, which is displayed in the VPN Policies table on the **VPN > Settings** page. You can customize the GroupVPN policy on the **VPN > Settings** page. If you uncheck Create Group VPN, the GroupVPN policy is removed from the **VPN > Settings** page.

**Step 4** Click the **Wireless** tab.



**Step 5** In the **Wireless Settings** section, check **Only allow traffic generated by a SonicPoint** to allow only traffic from SonicWALL SonicPoints to enter the WLAN Zone interface. This allows maximum security of your WLAN. Uncheck this option if you want to allow any traffic on your WLAN Zone regardless of whether or not it is from a wireless connection.



**Tip**

Uncheck **Only allow traffic generated by a SonicPoint** and use the zone on a wired interface to allow guest services on that interface.

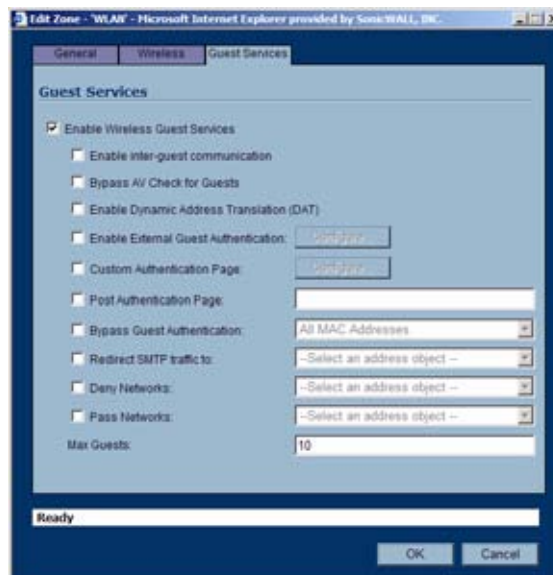
**Step 6** Select **SSL-VPN Enforcement** to require that all traffic that enters into the WLAN Zone be authenticated through a SonicWALL SSL-VPN appliance. If you select both **SSL-VPN Enforcement**, and **WiFiSec Enforcement**, the Wireless zone will allow traffic authenticated by either a SSL-VPN or an IPsec VPN.

**Step 7** In the **SSL-VPN Server** list, select an address object to direct traffic to the SonicWALL SSL-VPN appliance. You can select:

- **Create new address object...**
- Default Gateway
- Secondary Default Gateway
- X0 IP
- X1 IP
- X2 IP
- X3 IP
- X4 IP

– X5 IP

- Step 8** In the **SSL-VPN Service** list, select the service or group of services you want to allow for clients authenticated through the SSL-VPN.
- Step 9** Select **WiFiSec Enforcement** to require that all traffic that enters into the WLAN Zone interface be either IPsec traffic, WPA traffic, or both. With **WiFiSec Enforcement** enabled, all non-guest wireless clients connected to SonicPoints attached to an interface belonging to a Zone on which WiFiSec is enforced are required to use the strong security of IPsec. The VPN connection inherent in WiFiSec terminates at the “WLAN GroupVPN”, which you can configure independently of “WAN GroupVPN” or other Zone GroupVPN instances. If you select both **WiFiSec Enforcement**, and **SSL-VPN Enforcement**, the Wireless zone will allow traffic authenticated by either a SSL-VPN or an IPsec VPN.
- Step 10** If you have enabled **WiFiSec Enforcement**, you can specify services that are allowed to bypass the WiFiSec enforcement by checking **WiFiSec Exception Service** and then selecting the service you want to exempt from WiFiSec enforcement.
- Step 11** If you have enabled **WiFiSec Enforcement**, you can select **Require WiFiSec for Site-to-Site VPN Tunnel Traversal** to require WiFiSec security for all wireless connections through the WLAN zone that are part of a site-to-site VPN.
- Step 12** Select **Trust WPA traffic as WiFiSec** to accept WPA as an allowable alternative to IPsec. Both WPA-PSK (Pre-shared key) and WPA-EAP (Extensible Authentication Protocol using an external 802.1x/EAP capable RADIUS server) will be supported on SonicPoints.
- Step 13** Under the **SonicPoint Settings** heading, select the **SonicPoint Provisioning Profile** you want to apply to all SonicPoints connected to this zone. Whenever a SonicPoint connects to this zone, it will automatically be provisioned by the settings in the SonicPoint Provisioning Profile, unless you have individually configured it with different settings.
- Step 14** Click the **Guest Services** tab. You can choose from the following configuration options for Wireless Guest Services:



- **Enable Wireless Guest Services** - Enables guest services on the WLAN zone.
- **Enable inter-guest communication** - Allows guests connecting to SonicPoints in this WLAN Zone to communicate directly and wirelessly with each other.
- **Bypass AV Check for Guests** - Allows guest traffic to bypass Anti-Virus protection.

- **Enable Dynamic Address Translation (DAT)** - Wireless Guest Services (WGS) provides spur of the moment “hotspot” access to wireless-capable guests and visitors. For easy connectivity, WGS allows wireless users to authenticate and associate, obtain IP settings from the TZ 170 Wireless DHCP services, and authenticate using any web-browser. Without DAT, if a WGS user is not a DHCP client, but instead has static IP settings incompatible with the TZ 170 Wireless WLAN network settings, network connectivity is prevented until the user’s settings change to compatible values. Dynamic Address Translation (DAT) is a form of Network Address Translation (NAT) that allows the TZ 170 Wireless to support any IP addressing scheme for WGS users. For example, the TZ 170 Wireless WLAN interface is configured with its default address of 172.16.31.1, and one WGS client has a static IP Address of 192.168.0.10 and a default gateway of 192.168.0.1, while another has a static IP address of 10.1.1.10 and a gateway of 10.1.1.1, and DAT enables network communication for both of these clients.
- **Enable External Guest Authentication** - Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.

**Note**

Refer to the SonicWALL [Lightweight Hotspot Messaging](http://www.sonicwall.com/us/Support.html) Tech Note available at the SonicWALL documentation Web site <http://www.sonicwall.com/us/Support.html> for complete configuration of the **Enable External Guest Authentication** feature.

- **Custom Authentication Page** - Redirects users to a custom authentication page when they first connect to a SonicPoint in the WLAN zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
- **Post Authentication Page** - Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
- **Bypass Guest Authentication** - Allows a SonicPoint running WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another device upstream of the SonicPoint is enforcing authentication.
- **Redirect SMTP traffic to** - Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
- **Deny Networks** - Blocks traffic from the networks you name. Select the subnet, address group, or IP address to block traffic from.
- **Pass Networks** - Automatically allows traffic through the WLAN zone from the networks you select.
- **Max Guests** - Specifies the maximum number of guest users allowed to connect to the WLAN zone. The default is 10.

**Step 15** Click **OK** to apply these settings to the WLAN zone.



# CHAPTER 18

## Configuring DNS Settings

### Network > DNS

The Domain Name System (DNS) is a distributed, hierarchical system that provides a method for identifying hosts on the Internet using alphanumeric names called fully qualified domain names (FQDNs) instead of using difficult to remember numeric IP addresses.

The **Network > DNS** page allows you to manually configure your DNS settings, if necessary.



In the **DNS Settings** section, select **Specify DNS Servers Manually** and enter the IP address(es) into the DNS Server fields. Click **Apply** to save your changes.

To use the DNS Settings configured for the WAN zone, select **Inherit DNS Settings Dynamically from the WAN Zone**. Click **Apply** to save your changes.



The screenshot shows the 'Network > DNS' configuration window. The window title is 'Network > DNS' and it has 'Apply', 'Cancel', and '?' buttons. The main section is 'DNS Settings'. There are two radio button options: 'Specify DNS Servers Manually' (which is unselected) and 'Inherit DNS Settings Dynamically from WAN Zone' (which is selected). Under 'Specify DNS Servers Manually', there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', all containing '0.0.0.0'. Under 'Inherit DNS Settings Dynamically from WAN Zone', there are three input fields for 'DNS Server 1', 'DNS Server 2', and 'DNS Server 3', containing '10.2.16.6', '10.50.120.52', and '0.0.0.0' respectively.



## CHAPTER 19

# Configuring Address Objects

---

## Network > Address Objects

Address Objects are one of four object classes (Address, User, Service, and Schedule) in SonicOS Enhanced. These Address Objects allow for entities to be defined one time, and to be re-used in multiple referential instances throughout the SonicOS interface. For example, take an internal Web-Server with an IP address of 67.115.118.80. Rather than repeatedly typing in the IP address when constructing Access Rules or NAT Policies, Address Objects allow you to create a single entity called “My Web Server” as a Host Address Object with an IP address of 67.115.118.80. This Address Object, “My Web Server” can then be easily and efficiently selected from a drop-down menu in any configuration screen that employs Address Objects as a defining criterion.

## Types of Address Objects

Since there are multiple types of network address expressions, there are currently the following Address Objects types:

- **Host** – Host Address Objects define a single host by its IP address. The netmask for a Host Address Object will automatically be set to 32 bit (255.255.255.255) to identify it as a single host. For example, “My Web Server” with an IP address of “67.115.118.110” and a default netmask of “255.255.255.255”
- **Range** – Range Address Objects define a range of contiguous IP addresses. No netmask is associated with Range Address Objects, but internal logic generally treats each member of the specified range as a 32 bit-masked Host object. For example “My Public Servers” with an IP address starting value of “67.115.118.66” and an ending value of “67.115.118.90”. All 25 individual host addresses in this range would be comprised by this Range Address Object.
- **Network** – Network Address Objects are like Range objects in that they comprise multiple hosts, but rather than being bound by specified upper and lower range delimiters, the boundaries are defined by a valid netmask. Network Address Objects must be defined by the network’s address and a corresponding netmask. For example “My Public Network” with a Network Value of “67.115.118.64” and a Netmask of “255.255.255.224” would comprise addresses from 67.115.118.64 through to 67.115.118.95. As a general rule, the first address in a network (the network address) and the last address in a network (the broadcast address) are unusable.

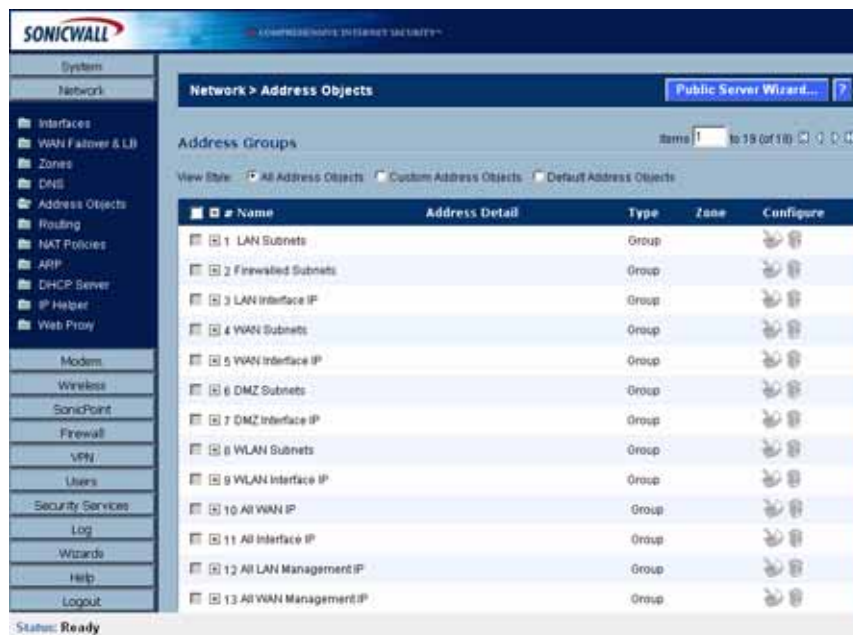
- **MAC Address** – MAC Address Objects allow for the identification of a host by its hardware address or MAC (Media Access Control) address. MAC Addresses are uniquely assigned to every piece of wired or wireless networking device by their hardware manufacturers, and are intended to be immutable. MAC addresses are 48 bit values that are expressed in 6 byte hex-notation. For example “My Access Point” with a MAC address of “00:06:01:AB:02:CD”. MAC Addresses are resolved to an IP address by referring to the ARP cache on the security appliance MAC Address objects are used by various components of Wireless configurations throughout SonicOS.
- **FQDN Address** – FQDN address objects allow for the identification of a host by its Fully Qualified Domain Names (FQDN), such as 'www.sonicwall.com'. FQDNs are resolved to their IP address (or IP addresses) using the DNS server configured on the security appliance. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

## Address Object Groups

SonicOS Enhanced has the ability to group Address Objects into Address Object Groups. Groups of Address Objects can be defined to introduce further referential efficiencies. Groups can comprise any combination of Host, Range, or Network Address Objects. MAC Address Objects should be grouped separately, although they can safely be added to Groups of IP-based Address Objects, where they will be ignored when their reference is contextually irrelevant (e.g. in a NAT Policy). For example “My Public Group” can contain Host Address Object “My Web Server” and Range Address Object “My Public Servers”, effectively representing IP Addresses 67.115.118.66 to 67.115.118.90 and IP Address 67.115.118.110.

## Creating and Managing Address Objects

The **Network > Address Objects** page allows you to create and manage your Address Objects.



You can view Address Objects in the following ways using the **View Style** menu:

- **All Address Objects** - displays all configured Address Objects.
- **Custom Address Objects** - displays Address Objects with custom properties.
- **Default Address Objects** - displays Address Objects configured by default on the SonicWALL security appliance.

Sorting Address Objects allows you to quickly and easily locate Address Objects configured on the SonicWALL security appliance.



**Note**

---

An Address Object must be defined before configuring NAT Policies, Access Rules, and Services.

---

## Navigating and Sorting the Address Objects and Address Groups Entries

The Address Objects and Address Groups tables provides easy pagination for viewing a large number of address objects and groups. You can navigate a large number of entries listed in the Address Objects or Address Groups tables by using the navigation control bar located at the top right of the tables. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

## Default Address Objects and Groups

The **Default Address Objects** view displays the default **Address Objects** and **Address Groups** for your SonicWALL security appliance. The **Default Address Objects** entries cannot be modified or deleted. Therefore, the **Notepad** (Edit) and **Trashcan** (delete) icons are dimmed.

#	Name	Address Detail	Type	Zone	Configure
1	LAN Primary IP	192.168.168.180/255.255.255.255	Host	LAN	[Dimmed Edit] [Dimmed Delete]
2	LAN Primary Subnet	192.168.168.0/255.255.255.0	Network	LAN	[Dimmed Edit] [Dimmed Delete]
3	WAN Primary IP	10.0.93.31/255.255.255.255	Host	WAN	[Dimmed Edit] [Dimmed Delete]
4	WAN Primary Subnet	10.0.93.0/255.255.255.0	Network	WAN	[Dimmed Edit] [Dimmed Delete]
5	OPT IP	172.16.32.1/255.255.255.255	Host	WLAN	[Dimmed Edit] [Dimmed Delete]
6	OPT Subnet	172.16.32.0/255.255.255.0	Network	WLAN	[Dimmed Edit] [Dimmed Delete]
7	Modem IP	0.0.0.0/255.255.255.255	Host	WAN	[Dimmed Edit] [Dimmed Delete]
8	Modem Subnet	0.0.0.0/0.0.0.0	Network	WAN	[Dimmed Edit] [Dimmed Delete]
9	WLAN IP	172.16.31.1/255.255.255.255	Host	WLAN	[Dimmed Edit] [Dimmed Delete]
10	WLAN Subnet	172.16.31.0/255.255.255.0	Network	WLAN	[Dimmed Edit] [Dimmed Delete]
11	Default Gateway	10.0.0.254/255.255.255.255	Host	WAN	[Dimmed Edit] [Dimmed Delete]
12	Secondary Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	[Dimmed Edit] [Dimmed Delete]
13	WLAN RemoteAccess Networks	0.0.0.0/0.0.0.0	Network	VPN	[Dimmed Edit] [Dimmed Delete]
14	Dial-Up Default Gateway	0.0.0.0/255.255.255.255	Host	WAN	[Dimmed Edit] [Dimmed Delete]
15	SonicPoint 00:02:6f:e0:09:72	00:02:6f:e0:09:72	MAC Address	WLAN	[Dimmed Edit] [Dimmed Delete]
16	Site_B	10.30.30.0/255.255.255.255	Host	LAN	[Dimmed Edit] [Dimmed Delete]
17	Access Point 00:06:b1:12:4b:a1	00:06:b1:12:4b:a1	MAC Address	WLAN	[Dimmed Edit] [Dimmed Delete]

## SonicWALL PRO 5060

### Default Address Objects

- X0 IP
- X0 Subnet
- X1 IP Host
- X1 Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP
- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- SonicPoint

## Default Address Groups

- LAN Subnets
- Firewalled Subnets
- LAN Interface IP
- WAN Subnets
- WAN Interface IP
- DMZ Subnets
- DMZ Interface IP
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- Custom Subnets
- Custom Interface IP
- All SonicPoints
- All Authorized Access Points
- WLAN Subnets
- WLAN Interface IP
- All SonicPoints
- All Authorized Access Points
- Node License Exclusion List
- RBL User White List
- RBL User Black List
- Default SonicPoint ACL Allow Group
- Default SonicPoint ACL Deny Group
- All X0 Management IP

## SonicWALL PRO 4060

### Default Address Objects

- LAN Primary IP
- LAN Primary Subnet
- WAN Primary IP
- WAN Primary Subnet
- X2 IP
- X2 Subnet
- X3 IP
- X3 Subnet
- X4 IP

- X4 Subnet
- X5 IP
- X5 Subnet
- Default Gateway
- Secondary Default Gateway
- WAN Remote Access Networks
- VPN DHCP Clients
- LAN Remote Access Networks
- SonicPoint

### **Default Address Groups**

- LAN Subnets
- Firewalled Subnets
- WAN Subnets
- DMZ Subnets
- ALL WAN IP
- All Interface IP
- All X0 Management IP
- All X1 Management IP
- All SonicPoints
- All Authorized Access Points
- LAN Interface IP
- WAN Interface IP
- DMZ Interface IP
- WLAN Subnets
- WLAN Interface IP
- Wireless2 Subnets
- Wireless2 Interface IP
- All SonicPoints
- All Authorized Access Points
- Node License Exclusion List
- RBL User White List
- RBL User Black List
- Default SonicPoint ACL Allow Group
- Default SonicPoint ACL Deny Group
- All X0 Management IP



## Adding an Address Object

To add an **Address Object**, click **Add** button under the **Address Objects** table in the **All Address Objects** or **Custom Address Objects** views to display the **Add Address Object** window.

**Step 1** Enter a name for the Network Object in the **Name** field.

**Step 2** Select **Host**, **Range**, **Network**, **MAC**, or **FQDN** from the **Type** menu.

- If you select **Host**, enter the IP address and netmask in the **IP Address** and **Netmask** fields.

- If you selected **Range**, enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.

- If you selected **Network**, enter the network IP address and netmask in the **Network** and **Netmask** fields.

- If you selected **MAC**, enter the MAC address and netmask in the **Network** and **MAC Address** field.


The screenshot shows a dialog box for adding an address object. The fields are: Name: 'Handheld1', Zone Assignment: 'WLAN', Type: 'MAC', and MAC Address: '00 00 00 1b a3 c1'. There is a checkbox for 'Subnetted host' which is checked. At the bottom, there is a 'Ready' field and 'OK' and 'Cancel' buttons.


- If you selected **FQDN**, enter the domain name for the individual site or range of sites (with a wildcard) in the **FQDN** field.

The screenshot shows a dialog box for adding an address object. The fields are: Name: 'All of Youtube', Zone Assignment: 'WAN', Type: 'FQDN', and FQDN Hostname: '\*.youtube.com'. At the bottom, there is a 'Ready' field and 'OK' and 'Cancel' buttons.

**Step 3** Select the zone to assign to the Address Object from the **Zone Assignment** menu.

## Editing or Deleting an Address Object

To edit an Address Object, click the edit icon  in the **Configure** column in the **Address Objects** table. The **Edit Address Object** window is displayed, which has the same settings as the **Add Address Object** window.

To delete an Address Object, click the Delete icon  in the **Configure** column for the Address Object you want to delete. A dialog box is displayed asking you to confirm the deletion. Click OK to delete the Address Object. To delete multiple active Address Objects, select them and click the **Delete** button.

## Creating Group Address Objects

As more and more Address Objects are added to the SonicWALL security appliance, you can simplify managing the addresses and access policies by creating groups of addresses. Changes made to the group are applied to each address in the group. To add a Group of Address Objects, click **Add Group** to display the **Add Address Object Group** window.



- 
- Step 1** Create a name for the group in the **Name** field.
  - Step 2** Select the Address Object from the list and click the right arrow. It is added to the group. Clicking while pressing the Ctrl key allows you to select multiple objects.
  - Step 3** Click **OK**.




### Tip

To remove an address or subnet from the group, select the IP address or subnet in the right column and click the left arrow. The selected item moves from the right column to the left column.

---

## Editing or Deleting Address Groups

To edit a group, click the edit icon  in the **Configure** column of the **Address Groups** table. The **Edit Address Object Group** window is displayed. Make your changes and then click **OK**.

To delete a group, click on the Delete icon  in the **Configure** column to delete an individual Address Group. A dialog box is displayed asking you to confirm the deletion. Click **OK** to delete the Address Group. To delete multiple active Address Groups, select them and click the **Delete** button.

## Public Server Wizard

SonicOS Enhanced includes the **Public Server Wizard** to automate the process of configuring the SonicWALL security appliance for handling public servers. For example, if you have an e-mail and Web server on your network for access from users on the Internet.



The **Public Server Wizard** allows you to select or define the server type (HTTP, FTP, Mail), the private (external) address objects, and the public (internal) address objects. Once the server type, private and public network objects are configured, the wizard creates the correct NAT Policies and Access Rule entries on the security appliance for the server. You can use the SonicWALL Management Interface for additional configuration options.

See **Part 13, Wizards** for more information on configuring the SonicWALL security appliance using wizards.

## Working with Dynamic Addresses

From its inception, SonicOS Enhanced has used Address Objects (AOs) to represent IP addresses in most areas throughout the user interface. Address Objects come in the following varieties:

- Host – An individual IP address, netmask and Zone association.
- MAC (original) – Media Access Control, or the unique hardware address of an Ethernet host. MAC AOs were originally introduced in SonicOS 2.5 and were used for:
  - Identifying SonicPoints
  - Allowing hosts to bypass Wireless Guest Services authentication
  - Authorizing the BSSID (Basic Service Set Identifier, or WLAN MAC) of wireless access points detected during wireless scans.

MAC AOs were originally not allowable targets in other areas of the management interface, such as Access Rules, so historically they could not be used to control a host's access by its hardware address.
- Range – A starting and ending IP address, inclusive of all addresses in between.
- Group – A collection of Address Objects of any assortment of types. Groups may contain other Groups, Host, MAC, Range, or FQDN Address Objects.

SonicOS Enhanced 3.5 redefined the operation of MAC AOs, and introduces Fully Qualified Domain Name (FQDN) AOs:

- MAC – SonicOS Enhanced 3.5 and higher will resolve MAC AOs to an IP address by referring to the ARP cache on the SonicWALL.
- FQDN – Fully Qualified Domain Names, such as 'www.reallybadwebsite.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the SonicWALL. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

While more effort is involved in creating an Address Object than in simply entering an IP address, AOs were implemented to complement the management scheme of SonicOS Enhanced, providing the following characteristics:

- Zone Association – When defined, Host, MAC, and FQDN AOs require an explicit Zone designation. In most areas of the interface (such as Access Rules) this is only used referentially. The functional application are the contextually accurate populations of Address Object drop-down lists, and the area of "VPN Access" definitions assigned to Users and Groups; when AOs are used to define VPN Access, the Access Rule auto-creation process refers to the AO's Zone to determine the correct intersection of VPN [Zone] for rule placement. In other words, if the "192.168.168.200 Host" Host AO, belonging to the LAN Zone was added to "VPN Access" for the "Trusted Users" User Group, the auto-created Access Rule would be assigned to the VPN LAN Zone.
- Management and Handling – The versatilely typed family of Address Objects can be easily used throughout the SonicOS Enhanced interface, allowing for handles (e.g. from Access Rules) to be quickly defined and managed. The ability to simply add or remove members from Address Object Groups effectively enables modifications of referencing rules and policies without requiring direct manipulation.
- Reusability – Objects only need to be defined once, and can then be easily referenced as many times as needed.

## Key Features of Dynamic Address Objects

The term Dynamic Address Object (DAO) describes the underlying framework enabling MAC and FQDN AOs. By transforming AOs from static to dynamic structures **Firewall > Access Rules** can automatically respond to changes in the network.



**Note**

The initial SonicOS Enhanced 4.0 release will only support Dynamic Address Objects within Access Rules. Future versions of SonicOS Enhanced might introduce DAO support to other subsystem, such as NAT, VPN, etc.

Feature	Benefit
FQDN wildcard support	<p>FQDN Address Objects support wildcard entries, such as “*.somedomainname.com”, by first resolving the base domain name to all its defined host IP addresses, and then by constantly actively gleaning DNS responses as they pass through the firewall.</p> <p>For example, creating an FQDN AO for “*.myspace.com” will first use the DNS servers configured on the firewall to resolve “myspace.com” to 63.208.226.40, 63.208.226.41, 63.208.226.42, and 63.208.226.43 (as can be confirmed by <i>nslookup myspace.com</i> or equivalent). Since most DNS servers do not allow zone transfers, it is typically not possible to automatically enumerate all the hosts in a domain. Instead, the SonicWALL will look for DNS responses <i>coming from sanctioned DNS servers</i> as they traverse the firewall. So if a host behind the firewall queries an external DNS server which is also a configured/defined DNS server on the SonicWALL, the SonicWALL will parse the response to see if it matches the domain of any wildcard FQDN AOs.</p> <p><b>Note</b> ‘Sanctioned’ DNS servers are those DNS servers configured for use by the SonicWALL firewall. The reason that responses from only sanctioned DNS servers are used in the wildcard learning process is to protect against the possibility of FQDN AO poisoning through the use of unsanctioned DNS servers with deliberately incorrect host entries. Future versions of SonicOS Enhanced might offer the option to support responses from all DNS server. The use of sanctioned DNS servers can be enforced with the use of Access Rules, as described later in the “Enforcing the use of sanctioned servers on the network” section.</p> <p>To illustrate, assume the firewall is configured to use DNS servers 4.2.2.1 and 4.2.2.2, and is providing these DNS servers to all firewalled client via DHCP. If firewalled client-A performs a DNS query against 4.2.2.1 or 4.2.2.2 for “vids.myspace.com”, the response will be examined by the firewall, and will be matched to the defined “*.myspace.com” FQDN AO. The result (63.208.226.224) will then be added to the resolved values of the “*.myspace.com” DAO.</p> <p><b>Note</b> If the workstation, client-A, in the example above had resolved and cached <i>vids.myspace.com</i> prior to the creation of the “*.myspace.com” AO, <i>vids.myspace.com</i> would not be resolved by the firewall because the client would use its resolver’s cache rather than issuing a new DNS request. As a result, the firewall would not have the chance to learn about <i>vids.myspace.com</i>, unless it was resolved by another host. On a Microsoft Windows workstation, the local resolver cache can be cleared using the command <b>ipconfig /flushdns</b>. This will force the client to resolve all FQDNs, allowing the firewall to learn them as they are accessed.</p> <p>Wildcard FQDN entries will resolve all hostnames within the context of the domain name, up to 256 entries per AO. For example, “*.sonicwall.com” will resolve <i>www.sonicwall.com</i>, <i>software.sonicwall.com</i>, <i>licensemanager.sonicwall.com</i>, to their respective IP addresses, but it will not resolve <i>sslvpn.demo.sonicwall.com</i> because it is in a different context; for <i>sslvpn.demo.sonicwall.com</i> to be resolved by a wildcard FQDN AO, the entry “*.demo.sonicwall.com” would be required, and would also resolve <i>sonicos-enhanced.demo.sonicwall.com</i>, <i>csm.demo.sonicwall.com</i>, <i>sonicos-standard.demo.sonicwall.com</i>, etc.</p> <p><b>Note</b> Wildcards only support full matches, not partial matches. In other words, “*.sonicwall.com” is a legitimate entry, but “w*.sonicwall.com”, “*w.sonicwall.com”, and “w*w.sonicwall.com” are not. A wildcard can only be specified once per entry, so “*.*.sonicwall.com”, for example, will not be functional.</p>

Feature	Benefit
FQDN resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the SonicWALL in the <b>Network &gt; DNS</b> page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.
FQDN entry caching	Resolved FQDN values will be cached in the event of resolution attempt failures subsequent to initial resolution. In other words, if "www.moosifer.com" resolves to 71.35.249.153 with a TTL of 300, but fails to resolve upon TTL expiry (for example, due to temporary DNS server unavailability), the 71.35.249.153 will be cached and used as valid until resolution succeeds, or until manually purged. Newly created FQDN entries that never successfully resolve, or entries that are purged and then fail to resolve will appear in an <b>unresolved</b> state.
MAC Address resolution using live ARP cache data	When a node is detected on any of the SonicWALL's physical segments through the ARP (Address Resolution Protocol) mechanism, the SonicWALL's ARP cache is updated with that node's MAC and IP address. When this update occurs, if a MAC Address Objects referencing that node's MAC is present, it will instantly be updated with the resolved address pairing. When a node times out of the ARP cache due to disuse (e.g. the host is no longer L2 connected to the firewall) the MAC AO will transition to an "unresolved" state.
MAC Address Object multi-homing support	MAC AOs can be configured to support multi-homed nodes, where multi-homed refers to nodes with more than one IP address per physical interface. Up to 256 resolved entries are allowed per AO. This way, if a single MAC address resolves to multiple IPs, all of the IP will be applicable to the Access Rules, etc. that refer to the MAC AO.
Automatic and manual refresh processes	MAC AO entries are automatically synchronized to the SonicWALL's ARP cache, and FQDN AO entries abide by DNS entry TTL values, ensuring that the resolved values are always fresh. In addition to these automatic update processes, manual Refresh and Purge capabilities are provided for individual DAOs, or for all defined DAOs.
FQDN resolution using DNS	FQDN Address Objects are resolved using the DNS servers configured on the SonicWALL in the <b>Network &gt; DNS</b> page. Since it is common for DNS entries to resolve to multiple IP addresses, the FQDN DAO resolution process will retrieve all of the addresses to which a host name resolves, up to 256 entries per AO. In addition to resolving the FQDN to its IPs, the resolution process will also associate the entry's TTL (time to live) as configured by the DNS administrator. TTL will then be honored to ensure the FQDN information does not become stale.

## Enforcing the use of sanctioned servers on the network

Although not a requirement, it is recommended to enforce the use of authorized or sanctioned servers on the network. This practice can help to reduce illicit network activity, and will also serve to ensure the reliability of the FQDN wildcard resolution process.

In general, it is good practice to define the endpoints of known protocol communications when possible. For example:

- Create Address Object Groups of sanctioned servers (e.g. SMTP, DNS, etc.)

31	Sanctioned DNS Servers	Group	
▶	10.50.195.3	10.50.195.3/255.255.255.255	Host LAN
▶	10.50.128.53	10.50.128.53/255.255.255.255	Host VPN
32	Sanctioned SMTP Servers	Group	
▶	10.50.195.2	10.50.195.2/255.255.255.255	Host LAN
▶	10.50.195.3	10.50.195.3/255.255.255.255	Host LAN

- Create Access Rules in the relevant Zones allowing only authorized SMTP servers on your network to communicate outbound SMTP; block all other outbound SMTP traffic to prevent intentional or unintentional outbound spamming.

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Sanctioned SMTP Servers	Any	SMTP (Send E-Mail)	Allow	All		<input checked="" type="checkbox"/>	
2	2	Any	Any	SMTP (Send E-Mail)	Deny	All		<input checked="" type="checkbox"/>	

- Create Access Rules in the relevant Zones allowing authorized DNS servers on your network to communicate with all destination hosts using DNS protocols (TCP/UDP 53). *Be sure to have this rule in place if you have DNS servers on your network, and you will be configuring the restrictive DNS rule that follows.*
- Create Access Rules in the relevant Zones allowing Firewalled Hosts to only communicate DNS (TCP/UDP 53) with sanctioned DNS servers; block all other DNS access to prevent communications with unauthorized DNS servers.

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Sanctioned DNS Servers	Any	DNS (Name Service)	Allow	All		<input checked="" type="checkbox"/>	
2	2	LAN Subnets	Sanctioned DNS Servers	DNS (Name Service)	Allow	All		<input checked="" type="checkbox"/>	
3	3	LAN Subnets	Any	DNS (Name Service)	Deny	All		<input checked="" type="checkbox"/>	

- Unsanctioned access attempts will then be viewable in the logs.

2	05/19/2006 14:52:26.738	Notice	Network Access	TCP connection dropped	10.50.195.28, 4372, LAN (admin)	71.32.231.227, 25, WAN	TCP SMTP (Send E-Mail)	<a href="#">2 (LAN-&gt;WAN)</a>
10	05/19/2006 14:51:32.608	Notice	Network Access	UDP packet dropped	10.50.195.28, 4336, LAN (admin)	4.2.2.1, 53, WAN	UDP DNS (Name Service) UDP	<a href="#">5 (LAN-&gt;WAN)</a>

## Using MAC and FQDN Dynamic Address Objects

MAC and FQDN DAOs provide extensive Access Rule construction flexibility. MAC and FQDN AOs are configured in the same fashion as static Address Objects, that is from the **Network > Address Objects** page. Once created, their status can be viewed by a mouse-over of their appearance, and log events will record their addition and deletion.

2	06/20/2006 00:13:39.064	Info	Firewall Event	Added host entry to dynamic address object	FQDN=* dyndns.org, TTL=60; Host=71.35.249.153			
---	-------------------------	------	----------------	--	---	--	--	--

Dynamic Address Objects lend themselves to many applications. The following are just a few examples of how they may be used. Future versions of SonicOS Enhanced may expand their versatility even further.



## Blocking All Protocol Access to a Domain using FQDN DAOs

There might be instances where you wish to block all protocol access to a particular destination IP because of non-standard ports of operations, unknown protocol use, or intentional traffic obscuration through encryption, tunneling, or both. An example would be a user who has set up an HTTPS proxy server (or other method of port-forwarding/tunneling on “trusted” ports like 53, 80, 443, as well as nonstandard ports, like 5734, 23221, and 63466) on his DSL or cable modem home network for the purpose of obscuring his traffic by tunneling it through his home network. The lack of port predictability is usually further complicated by the dynamic addressing of these networks, making the IP address equally unpredictable.

Since these scenarios generally employ dynamic DNS (DDNS) registrations for the purpose of allowing users to locate the home network, FQDN AOs can be put to aggressive use to block access to all hosts within a DDNS registrar.



**Note**

A DDNS target is used in this example for illustration. Non-DDNS target domains can be used just as well.

### Assumptions

- The SonicWALL firewall is configured to use DNS server 10.50.165.3, 10.50.128.53
- The SonicWALL is providing DHCP leases to all firewalled users. All hosts on the network use the configured DNS servers above for resolution.
  - DNS communications to unsanctioned DNS servers can optionally be blocked with Access Rules, as described in the ‘Enforcing the use of sanctioned servers on the network’ section.
- The DSL home user is registering the hostname *moosifer.dyndns.org* with the DDNS provider DynDNS. For this session, the ISP assigned the DSL connection the address *71.35.249.153*.
  - A wildcard FQDN AO is used for illustration because other hostnames could easily be registered for the same IP address. Entries for other DDNS providers could also be added, as needed.

### Step 1 – Create the FQDN Address Object

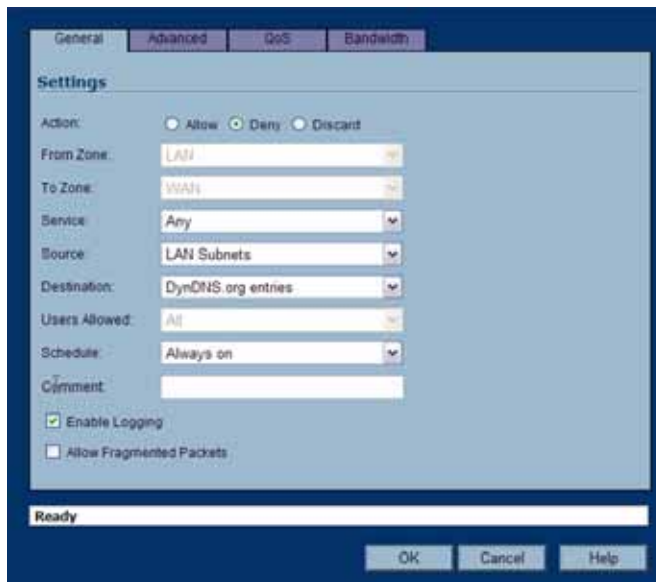
- From **Network > Address Objects**, select **Add** and create the following Address Object:

Name:	DynDNS.org entries
Zone Assignment:	WAN
Type:	FQDN
FQDN Hostname:	*dyndns.org
Ready	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

- When first created, this entry will resolve only to the address for dyndns.org, e.g. 63.208.196.110.

**Step 2 – Create the Firewall Access Rule**

- From the **Firewall > Access Rules** page, LAN->WAN Zone intersection, Add an Access Rule as follows:



**Note**

Rather than specifying 'LAN Subnets' as the source, a more specific source could be specified, as appropriate, so that only certain hosts are denied access to the targets.

- When a host behind the firewall attempts to resolve moosifer.dyndns.org using a sanctioned DNS server, the IP address(es) returned in the query response will be dynamically added to the FQDN AO.
- Any protocol access to target hosts within that FQDN will be blocked, and the access attempt will be logged:

3	06/20/2006 00:20:20.600	Notice	Network Access	TCP connection dropped	10.50.165.20, 1777, LAN (admin)	71.35.249.153, 443, WAN	TCP HTTPS	<a href="#">S (LAN-&gt;WAN)</a>
6	06/20/2006 00:23:22.256	Notice	Network Access	TCP connection dropped	10.50.165.25, 2234, LAN	71.35.249.153, 63446, WAN	TCP Port: 63446	<a href="#">S (LAN-&gt;WAN)</a>

**Using an Internal DNS Server for FQDN-based Access Rules**

It is common for dynamically configured (DHCP) network environments to work in combination with internal DNS servers for the purposes of dynamically registering internal hosts – a common example of this is Microsoft’s DHCP and DNS services. Hosts on such networks can easily be configured to dynamically update DNS records on an appropriately configured DNS server (for example, see the Microsoft Knowledgebase article “How to configure DNS dynamic updates in Windows Server 2003” at

<http://support.microsoft.com/kb/816592/en-us>).

The following illustrates a packet dissection of a typical DNS dynamic update process, showing the dynamically configured host *10.50.165.249* registering its full hostname *bohuymath.moosifer.com* with the (DHCP provided) DNS server *10.50.165.3*:

```

19 2.100829 10.50.165.249 2420 10.50.165.3 53 DNS Dynamic update SOA moosifer.com
20 2.105100 10.50.165.3 53 10.50.165.249 2420 DNS Dynamic update response CNAME A 10.50.165.249
# Frame 19 (122 bytes on wire, 122 bytes captured)
# Ethernet II, Src: 00:00:00:1b:e3:cf (00:00:00:1b:e3:cf), Dst: 00:00:00:18:43:00 (00:00:00:18:43:00)
# Internet Protocol, Src: 10.50.165.249 (10.50.165.249), Dst: 10.50.165.3 (10.50.165.3)
# User Datagram Protocol, Src Port: 2420 (2420), Dst Port: 53 (53)
# Domain Name System (query)
  Transaction ID: 0x0bad
  # Flags: 0x2800 (Dynamic update)
    0... .. = Response: Message is a query
    .010 1... .. = Opcode: dynamic update (5)
    .... .0. .... = Truncated: Message is not truncated
    .... .0 .... = Recursion desired: Don't do query recursively
    .... .0.. .... = Z: reserved (0)
    .... ..0 .... = Non-authenticated data OK: Non-authenticated data is unacceptable
  Zones: 1
  Prerequisites: 2
  updates: 0
  Additional RRS: 0
  # Zone
    # moosifer.com: type SOA, class IN
      Name: moosifer.com
      Type: SOA (Start of zone of authority)
      Class: IN (0x0001)
  # Prerequisites
    # bohuymath.moosifer.com: type CNAME, class NONE
      Name: bohuymath.moosifer.com
      type: CNAME (canonical name for an alias)
      class: NONE (0x00fe)
      time to live: 0 time
      Data length: 0
    # bohuymath.moosifer.com: type A, class IN, addr 10.50.165.249
      Name: bohuymath.moosifer.com
      Type: A (Host address)
      Class: IN (0x0001)
      Time to live: 0 time
      Data length: 4
      Addr: 10.50.165.249

```

In such environments, it could prove useful to employ FQDN AOs to control access by hostname. This would be most applicable in networks where hostnames are known, such as where hostname lists are maintained, or where a predictable naming convention is used.

## Controlling a Dynamic Host's Network Access by MAC Address

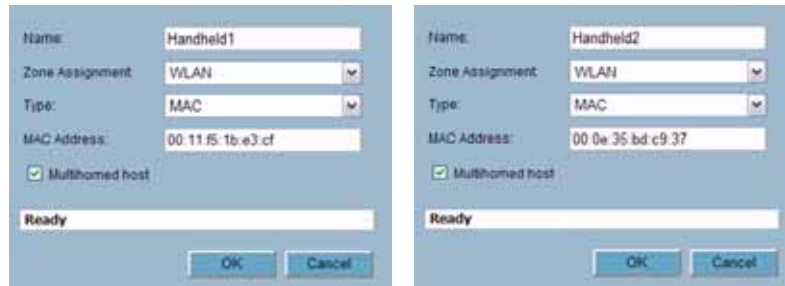
Since DHCP is far more common than static addressing in most networks, it is sometimes difficult to predict the IP address of dynamically configured hosts, particularly in the absence of dynamic DNS updates or reliable hostnames. In these situations, it is possible to use MAC Address Objects to control a host's access by its relatively immutable MAC (hardware) address.

Like most other methods of access control, this can be employed either inclusively, for example, to deny access to/for a specific host or group of hosts, or exclusively, where only a specific host or group of hosts are granted access, and all other are denied. In this example, we will illustrate the latter.

Assuming you had a set of DHCP-enabled wireless clients running a proprietary operating system which precluded any type of user-level authentication, and that you wanted to only allow these clients to access an application-specific server (e.g. 10.50.165.2) on your LAN. The WLAN segment is using WPA-PSK for security, and this set of clients should only have access to the 10.50.165.2 server, but to no other LAN resources. All other wireless clients should not be able to access the 10.50.165.2 server, but should have unrestricted access everywhere else.

**Step 1 – Create the MAC Address Objects**

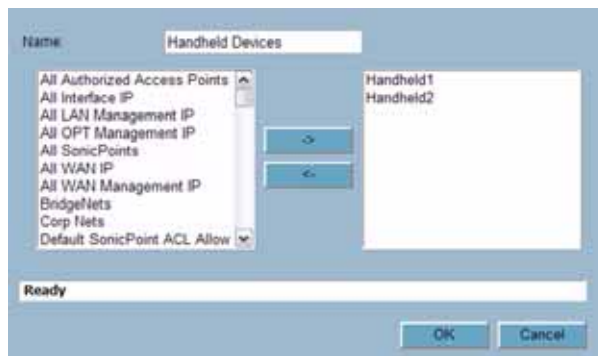
- From **Network > Address Objects**, select **Add** and create the following Address Object (multi-homing optional, as needed):



- Once created, if the hosts were present in the SonicWALL's ARP cache, they will be resolved immediately, otherwise they will appear in an *unresolved* state until they are activated and are discovered through ARP:

<input type="checkbox"/>	29	Handheld1	00:11:15:1b:00:00	MAC Address	WLAN		
<input type="checkbox"/>	30	Handheld2	0:0e:35:bd:00:00	MAC Address	WLAN		

- Create an Address Object Group comprising the Handheld devices:



**Step 2 – Create the Firewall Access Rules**

- From the **Firewall > Access Rules** page, WLAN->LAN Zone intersection, add Access Rules as follows:

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
<input type="checkbox"/>	1	Handheld Devices	10.50.165.3	MediaMoose Services	Allow	All		<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2	Any	10.50.165.3	MediaMoose Services	Deny	All		<input checked="" type="checkbox"/>	
<input type="checkbox"/>	3	Handheld Devices	Any	Any	Deny	All		<input checked="" type="checkbox"/>	
<input type="checkbox"/>	4	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	



**Note**

The 'MediaMoose Services' service is used to represent the specific application used by the handheld devices. The declaration of a specific service is optional, as needed.

## Bandwidth Managing Access to an Entire Domain

Streaming media is one of the most profligate consumers of network bandwidth. But trying to control access, or manage bandwidth allotted to these sites is difficult because most sites that serve streaming media tend to do so off of large server farms. Moreover, these sites frequently re-encode the media and deliver it over HTTP, making it even more difficult to classify and isolate. Manual management of lists of servers is a difficult task, but wildcard FQDN Address Objects can be used to simplify this effort.

### Step 1 – Create the FQDN Address Object

- From **Network > Address Objects**, select **Add** and create the following Address Object:

The screenshot shows a dialog box for creating a new Address Object. The fields are as follows:

Name:	All of Youtube
Zone Assignment:	WAN
Type:	FQDN
FQDN Hostname:	*.youtube.com
Status:	Ready

Buttons for 'OK' and 'Cancel' are visible at the bottom right.

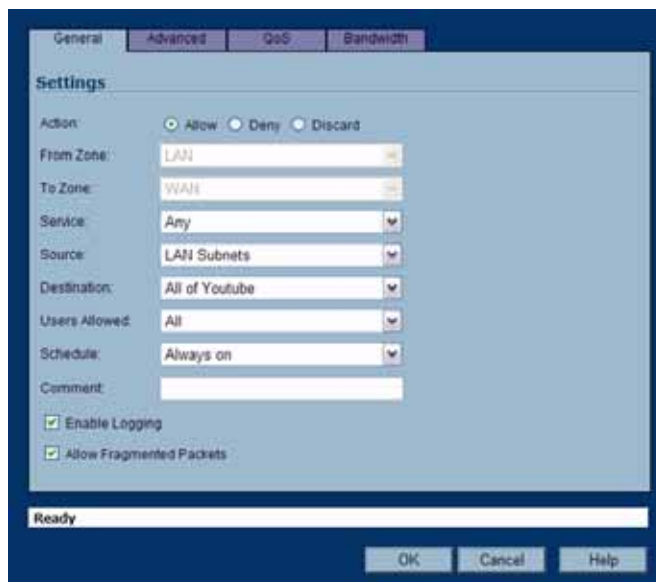
Upon initial creation, youtube.com will resolve to IP addresses 208.65.153.240, 208.65.153.241, 208.65.153.242, but after an internal host begins to resolve hosts for all of the elements within the youtube.com domain, the learned host entries will be added, such as the entry for the v87.youtube.com server (208.65.154.84):

Name	Zone Assignment	Type	Hosts	Action	Zone	Priority	Icon	Icon	Icon
LAN Subnets				Allow	All				
All of Youtube				Allow	All				
<b>Address Properties</b>									
Host: 208.65.153.240; TTL=144									
Host: 208.65.153.241; TTL=144									
Host: 208.65.153.242; TTL=144									
Host: 208.65.154.84; TTL=300									

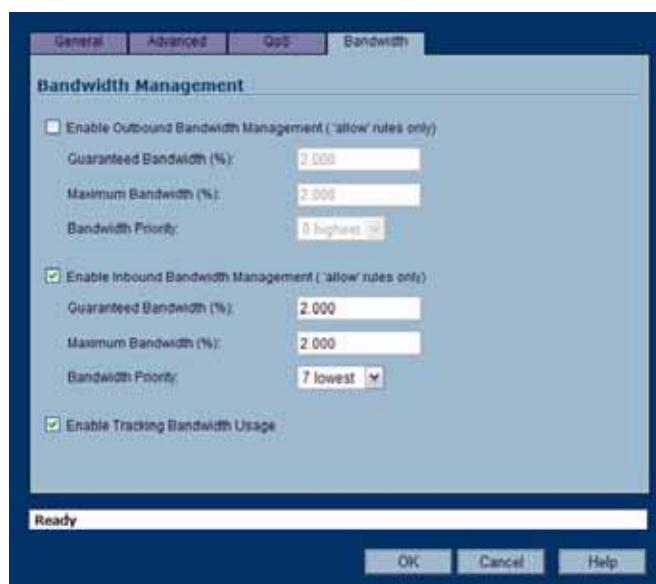
Buttons for 'Add' and 'Restore Defaults' are visible at the bottom.

**Step 2 – Create the Firewall Access Rule**

- From the **Firewall > Access Rules** page, LAN->WAN Zone intersection, add an Access Rule as follows:



The screenshot shows the 'Settings' tab of the Firewall Access Rule configuration window. The 'Action' is set to 'Allow'. The 'From Zone' is 'LAN' and the 'To Zone' is 'WAN'. The 'Service' is 'Any', 'Source' is 'LAN Subnets', and 'Destination' is 'All of Youtube'. 'Users Allowed' is 'All' and 'Schedule' is 'Always on'. There is a 'Comment' field. The 'Enable Logging' and 'Allow Fragmented Packets' checkboxes are checked. The status bar shows 'Ready' and buttons for 'OK', 'Cancel', and 'Help'.



The screenshot shows the 'Bandwidth Management' tab of the Firewall Access Rule configuration window. The 'Enable Outbound Bandwidth Management' checkbox is unchecked. The 'Guaranteed Bandwidth (%)' is 2,000 and the 'Maximum Bandwidth (%)' is 2,000. The 'Bandwidth Priority' is '0 highest'. The 'Enable Inbound Bandwidth Management' checkbox is checked. The 'Guaranteed Bandwidth (%)' is 2,000 and the 'Maximum Bandwidth (%)' is 2,000. The 'Bandwidth Priority' is '7 lowest'. The 'Enable Tracking Bandwidth Usage' checkbox is checked. The status bar shows 'Ready' and buttons for 'OK', 'Cancel', and 'Help'.

**Note**

If you do not see the Bandwidth tab, you can enable bandwidth management by declaring the bandwidth on your WAN interfaces. For more information on BWM, refer to the Configuring QoS and BWM document at: [http://www.sonicwall.com/support/pdfs/configuring\\_qos\\_and\\_bwm.pdf](http://www.sonicwall.com/support/pdfs/configuring_qos_and_bwm.pdf)

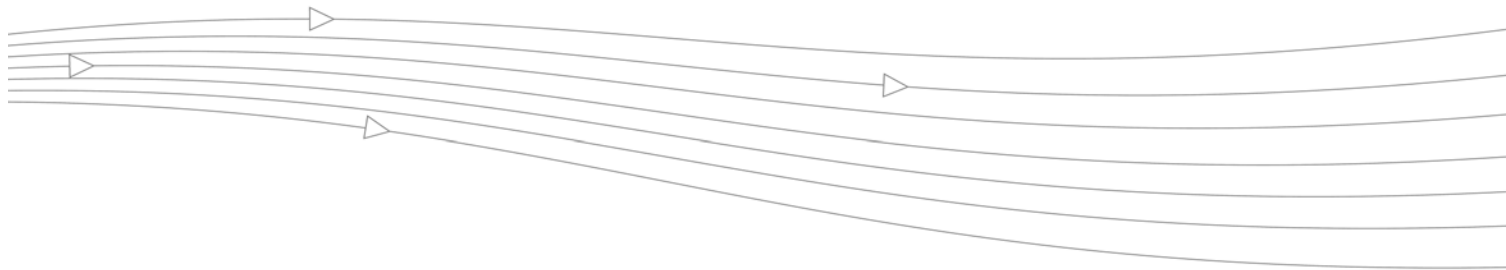
- The BWM icon will appear within the Access Rule table indicating that BWM is active, and providing statistics:



- Access to all \*.youtube.com hosts, using any protocol, will now be cumulatively limited to 2% of your total available bandwidth for all user sessions.







# CHAPTER 20

## Configuring Routes

### Network > Routing

If you have routers on your interfaces, you can configure static routes on the SonicWALL security appliance on the **Network > Routing** page. You can create static routing policies that create static routing entries that make decisions based upon source address, source netmask, destination address, destination netmask, service, interface, gateway and metric. This feature allows for full control of forwarding based upon a large number of user-defined variables.

Interface (Zone)	Status	Configure
LAN (LAN)	Disabled	
WAN (WAN)	Disabled	
OPT (WLAN)	Disabled	
Modem (WAN)	Disabled	
WLAN (WLAN)	Disabled	

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	255.255.255.255/32	Any	0.0.0.0	LAN	20	1		
2	Any	Default Gateway	Any	0.0.0.0	WAN	20	2		
3	Any	LAN Primary Subnet	Any	0.0.0.0	LAN	20	3		
4	Any	OPT Subnet	Any	0.0.0.0	OPT	20	4		
5	Any	WLAN Subnet	Any	0.0.0.0	WLAN	20	5		
6	Any	WAN Primary Subnet	Any	0.0.0.0	WAN	20	6		
7	Any	OPT DAT Subnet	Any	0.0.0.0	OPT	20	7		
8	Any	WLAN DAT Subnet	Any	0.0.0.0	WLAN	20	8		
9	WAN Primary Subnet	Any	Any	Default Gateway	WAN	20	9		
10	Any	0.0.0.0/0	Any	10.0.0.254	WAN	20	10		

## Route Advertisement

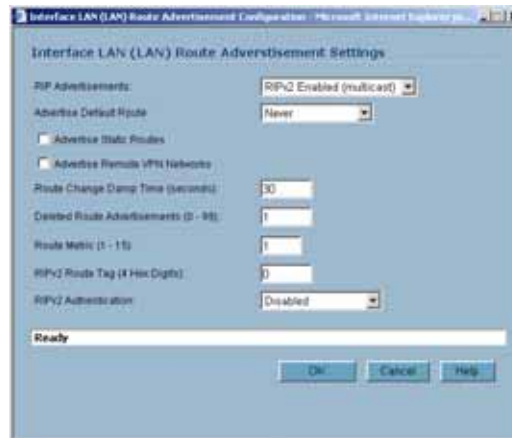
The SonicWALL security appliance uses RIPv1 or RIPv2 to advertise its static and dynamic routes to other routers on the network. Changes in the status of VPN tunnels between the SonicWALL security appliance and remote VPN gateways are also reflected in the RIPv2 advertisements. Choose between RIPv1 or RIPv2 based on your router's capabilities or configuration. RIPv1 is an earlier version of the protocol that has fewer features, and it also sends packets via broadcast instead of multicast. RIPv2 packets are backwards-compatible and can be accepted by some RIPv1 implementations that provide an option of listening for multicast packets. The RIPv2 Enabled (broadcast) selection broadcasts packets instead of multicasting packets is for heterogeneous networks with a mixture of RIPv1 and RIPv2 routers.

Interface (Zone)	Status	Configure
LAN (LAN)	Disabled	
WAN (WAN)	Disabled	
GFT (WLAN)	Disabled	
Modem (WAN)	Disabled	
WLAN (WLAN)	Disabled	

## Route Advertisement Configuration

To enable Route Advertisement for an Interface, follow these steps:

- Step 1** Click the **Notepad** icon in the **Configure** column for the interface. The **Route Advertisement Configuration** window is displayed.



- Step 2** Select one of the following types of RIP Advertisements:
- **RIPv1 Enabled** - RIPv1 is the first version of Routing Information Protocol.
  - **RIPv2 Enabled (multicast)** - To send route advertisements using multicasting (a single data packet to specific nodes on the network).

- **RIPv2 Enabled (broadcast)** - To send route advertisements using broadcasting (a single data packet to all nodes on the network).
- Step 3** In the **Advertise Default Route** menu, select **Never**, or **When WAN is up**, or **Always**.
- Step 4** Enable **Advertise Static Routes** if you have static routes configured on the SonicWALL security appliance, enable this feature to exclude them from Route Advertisement.
- Step 5** Enable **Advertise Remote VPN Networks** if you want to advertise VPN networks.
- Step 6** Enter a value in seconds between advertisements broadcasted over a network in the **Route Change Damp Time (seconds)** field. The default value is **30** seconds. A lower value corresponds with a higher volume of broadcast traffic over the network. The **Route Change Damp Time (seconds)** setting defines the delay between the time a VPN tunnel changes state (up or down) and the time the change is advertised with RIP. The delay, in seconds, prevents ambiguous route advertisements sent as a result of temporary change in the VPN tunnel status.
- Step 7** Enter the number of advertisements that a deleted route broadcasts until it stops in the **Deleted Route Advertisements (0-99)** field. The default value is **1**.
- Step 8** Enter a value from 1 to 15 in the **Route Metric (1-15)** field. This is the number of times a packet touches a router from the source IP address to the destination IP address.
- Step 9** If RIPv2 is selected from the Route Advertisements menu, you can enter a value for the route tag in the **RIPv2 Route Tag (4 HEX Digits)** field. This value is implementation-dependent and provides a mechanism for routers to classify the originators of RIPv2 advertisements. This field is optional.
- Step 10** If you want to enable RIPv2 authentication, select one of the following options from the **RIPv2 Authentication** menu:
- **User defined** - Enter 4 hex digits in the Authentication Type (4 hex digits) field. Enter 32 hex digits in the Authentication Data (32 Hex Digits) field.
  - **Cleartext Password** - Enter a password in the Authentication Password (Max 16 Chars) field. A maximum of 16 characters can be used to define a password.
  - **MD5 Digest** - Enter a numerical value from 0-255 in the Authentication Key-Id (0-255) field. Enter a 32 hex digit value for the Authentication Key (32 hex digits) field, or use the generated key.
- Step 11** Click **OK**.

## Route Policies

SonicOS Enhanced provides Policy Based Routing (PBR) to provide more flexible and granular traffic handling capabilities.

## Policy Based Routing

A simple static routing entry specifies how to handle traffic that matches specific criteria, such as destination address, destination mask, gateway to forward traffic, the interface that gateway is located, and the route metric. This method of static routing satisfies most static requirements, but is limited to forwarding based only on destination addressing.

Policy Based Routing (PBR) allows you to create extended static routes to provide more flexible and granular traffic handling capabilities. SonicOS Enhanced PBR allows for matching based upon source address, source netmask, destination address, destination netmask, service, interface, and metric. This method of routing allows for full control of forwarding based upon a large number of user defined variables.

A metric is a weighted cost assigned to static and dynamic routes. Metrics have a value between 0 and 255. Lower metrics are considered better and take precedence over higher costs. SonicOS Enhanced adheres to Cisco defined metric values for directly connected interfaces, statically encoded routes, and all dynamic IP routing protocols.

Metric Value	Description
1	Static Route
5	EIGRP Summary
20	External BGP
90	EIGRP
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	EGP
170	External EIGRP
Internal	BGP

## Route Policies Table

You can change the view your route policies in the **Route Policies** table by selecting one of the view settings in the **View Style** menu.

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	255.255.255.0/24	Any	0.0.0.0	LAN	20	1		
2	Any	Default Gateway	Any	0.0.0.0	WAN	30	2		
3	Any	LAN Primary Subnet	Any	0.0.0.0	LAN	20	3		
4	Any	OPT Subnet	Any	0.0.0.0	OPT	20	4		
5	Any	WLAN Subnet	Any	0.0.0.0	WLAN	20	5		
6	Any	WAN Primary Subnet	Any	0.0.0.0	WAN	20	6		
7	Any	OPT DAT Subnet	Any	0.0.0.0	OPT	20	7		
8	Any	WLAN DAT Subnet	Any	0.0.0.0	WLAN	20	8		
9	WAN Primary Subnet	Any	Any	Default Gateway	WAN	20	9		
10	Any	0.0.0.0/0	Any	10.0.0.254	WAN	20	10		

**All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **Route Policies** table provides easy pagination for viewing a large number of routing policies. You can navigate a large number of routing policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific routing policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

## A Route Policy Example

The following example walks you through creating a route policy for two simultaneously active WAN interfaces. For this example, a secondary WAN interface needs to be setup on the **OPT** interface and configured with the settings from your ISP. Next, configure the security appliance for load balancing by checking the **Enable Load Balancing** on the **Network > WAN Failover & LB** page. For this example, choose **Per Connection Round-Robin** as the load balancing method in the **Network > WAN Failover & LB** page. Click **Apply** to save your changes on the **Network > WAN Failover & LB** page.

- Step 1** Click the **Add** button under the Route Policies table. The **Add Route Policy** window is displayed.



- Step 2** Create a routing policy that directs all **LAN Subnet** sources to **Any** destinations for **HTTP** service out of the **Default Gateway** via the **WAN** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force http out primary** into the **Comment** field. Click **OK**.
- Step 3** Create a second routing policy that directs all **LAN Subnet** sources to **Any** destinations for **Telnet** service out of the **Secondary Default Gateway** via the **Opt** interface by selecting these settings from the **Source**, **Destination**, **Service**, **Gateway** and **Interface** menus respectively. Use the default **1** in the **Metric** field and enter **force telnet out backup** into the **Comment** field. Click **OK**.

These two policy-based routes force all sources from the LAN subnet to always go out the primary WAN when using any HTTP-based application, and forces all sources from the LAN subnet to always go out the backup WAN when using any Telnet-based application.

To test the HTTP policy-based route, from a computer attached to the LAN interface, access the public Web site <http://www.whatismyip.com> and <http://whatismyip.everdot.org>. Both sites display the primary WAN interface's IP address and not the secondary WAN interface.

To test the Telnet policy-based route, telnet to route-server.exodus.net and when logged in, issue the *who* command. It displays the IP address (or resolved FQDN) of the WAN IP address of the secondary WAN interface and not the primary WAN interface.

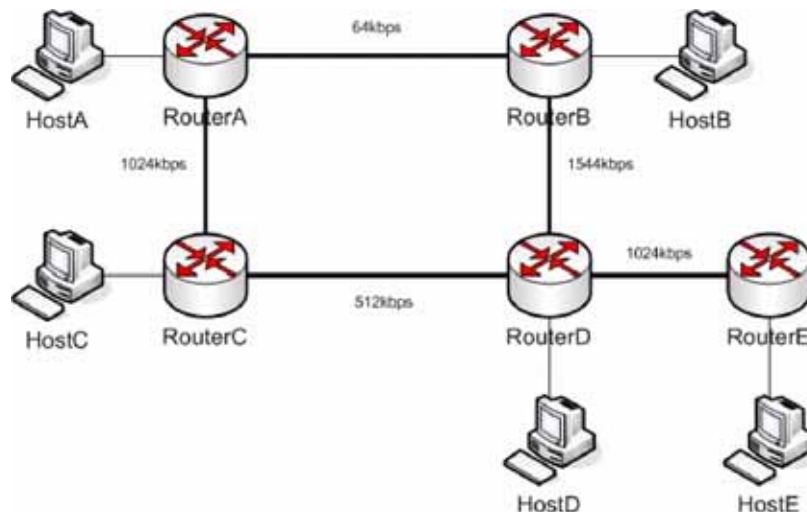
## Advanced Routing Services (OSPF and RIP)

In addition to Policy Based Routing and RIP advertising, SonicOS Enhanced offers the option of enabling Advanced Routing Services (ARS). Advanced Routing Services provides full advertising and listening support for the Routing Information Protocol (RIPv1 - RFC1058) and (RIPv2 - RFC2453), and Open Shortest Path First (OSPFv2 – RFC2328). Advanced Routing Service should only be enabled by those environments requiring support for either or both of these dynamic routing protocols.

RIP and OSPF are Interior Gateway Protocols (IGP) that are both widely used by networks of various sizes to automate the process of route distribution. RIP is commonly used within smaller networks, while OSPF is used by larger networks, although network size should not be the only factor used to determine the appropriateness of one protocol over the other – network speed, interoperability requirements, and relative overall complexity, for example, should also be considered. RIPv1 and RIPv2 are both supported by ARS, the largest differences between the two being that RIPv2 supports VLSM (Variable Length Subnet Masks), authentication, and routing updates. The following table illustrates the major differences between RIPv1, RIPv2, and OSPFv2:

	RIPv1	RIPv2	OSPFv2
Protocol metrics	Distance Vector	Distance Vector	Link State
Maximum Hops	15	15	Unlimited
Routing table updates	Full table broadcast periodically, slower convergence	Full table broadcast or multicast periodically, slower convergence	Link state advertisement multicasts, triggered by changes, fast convergence
Subnet Sizes Supported	Only class-based (a/b/c) subnets support	Class-based only	VLSM
Autonomous system topology	Indivisible and flat	Indivisible and flat	Area based, allowing for segmentation and aggregation

- Protocol Type – Distance Vector protocols such as RIP base routing metrics exclusively on hop counts, while Link state protocols such as OSPF consider the state of the link when determining metrics. For example, OSPF determines interface metrics by dividing its reference bandwidth (100mbits by default) by the interface speed – the faster the link, the lower the cost and the more preferable the path. Consider the following example network:



In the above sample network, if Host A wanted to reach Host B, with RIP, the lowest cost route would be from Router A to Router B, across the relatively slow 64kbps link. With OSPF, the cost from Router A to Router B would be 1562, while the cost from Router A to Router C to Router D to Router B would be 364 (see the Cost section in OSPF concepts later), making it the preferred route.

- Maximum Hops – RIP imposes a hop count of 15 to help prevent routing loops which can occur when bad (e.g. stale) routing information is broadcast and propagated through a network either due to misconfiguration, or slow convergence. Consider if the link between Router D and Router E failed in the diagram above, and there were no safeguards in place:
- Router A's routing information states that it can reach Network E through Router B or Router C with a metric of 3.
- When the link between Router D and Router E fail, and Router A broadcasts its routing information, Router B and Router C determine that they can reach Network E through Router A with a metric of 4.
- Router B and Router C broadcast this information, and it is received by Router D which then determines it can reach Network E through Router B or Router C with a metric of 5.
- This loop continues until the hop count of 16 (infinity) is reached.

Other measures against this sort of situation are also commonly employed by RIP, including:

- Split-Horizon – A preventative mechanism where routing information learned through an interface is not sent back out the same interface. This generally works well on broadcast links, but not on non-broadcast links such as Frame Relay, where a single link can commonly be used to reach two separate autonomous systems.
- Poison reverse – Also known as route poisoning, an extension of split-horizon where a network is advertised with a metric of 16 (unreachable), helping to ensure that incorrect alternative routes aren't propagated.

OSPF does not have to impose a hop count limit because it does not advertise entire routing tables, rather it generally only sends link state updates when changes occur. This is a significant advantage in larger networks in that it converges more quickly, produces less update traffic, and supports an unlimited number of hops.

- Routing table updates – As mentioned above, the practice of sending an entire routing table introduces the problems of slower convergences, higher bandwidth utilization, and increased potential for stale routing information. RIPv1 broadcasts its entire routing table at a prescribed interval (usually every 30 seconds), RIPv2 can either broadcast or multicast, and OSPF multicasts only link state updates whenever a change to the network fabric occurs. OSPF has a further advantage of using designated routers (DR) in forming adjacencies in multiple-access networks (more on these concepts later) so that updates don't have to be sent to the entire network.
- Subnet sizes supported – RIPv1 was first implemented when networks were strictly class A, class B, and class C (and later D and E):
- Class A – 1.0.0.0 to 126.0.0.0 (0.0.0.0 and 127.0.0.0 are reserved)
  - Leftmost bit 0; 7 network bits; 24 host bits
  - 0nnnnnnn hhhhhhhh hhhhhhhh hhhhhhhh (8 bit classful netmask)
  - 126 Class A networks, 16,777,214 hosts each
- Class B - 128.0.0.0 to 191.255.0.0
  - Leftmost bits 10; 14 network bits; 16 host bits
  - 10nnnnnn nnnnnnnn hhhhhhhh hhhhhhhh (16 bit classful netmask)
  - 16,384 Class B networks, 65,532 hosts each
- Class C – 192.0.0.0 to 223.255.255.0
  - Leftmost bits 110; 21 network bits; 8 host bits
  - 110nnnnn nnnnnnnn nnnnnnnn hhhhhhhh (24 bit classful netmask)
  - 2,097,152 Class Cs networks, 254 hosts each
- Class D - 224.0.0.0 to 239.255.255.255 (multicast)
  - Leftmost bits 1110; 28 multicast address bits
  - 1110mmmm mmmmmmmm mmmmmmmm mmmmmmmm
- Class E - 240.0.0.0 to 255.255.255.255 (reserved)
  - Leftmost bits 1111; 28 reserved address bits
  - 1111rrrr rrrrrrrr rrrrrrrr rrrrrrrr

This method of address allocation proved to be very inefficient because it provided no flexibility, neither in the way of segmentation (subnetting) or aggregation (supernetting, or CIDR – classless inter-domain routing) by means of VLSM – variable length subnet masks.

VLSM, supported by RIPv2 and OSPF, allows for classless representation of networks to break larger networks into smaller networks:

For example, take the classful 10.0.0.0/8 network, and assign it a /24 netmask. This subnetting allocates an additional 16 bits from the host range to the network range (24-8=16). To calculate the number of additional networks this subnetting provides, raise 2 to the number of additional bits:  $2^{16}=65,536$ . Thus, rather than having a single network with 16.7 million hosts (usually more than most LAN's require) it is possible to have 65,536 networks, each with 254 usable hosts.

VLSM also allows for route aggregation (CIDR):



For example, if you had 8 class C networks: 192.168.0.0/24 through 192.168.7.0/24, rather than having to have a separate route statement to each of them, it would be possible to provide a single route to 192.168.0.0/21 which would encompass them all.

This ability, in addition to providing more efficient and flexible allocation of IP address space, also allows routing tables and routing updates to be kept smaller.

- Autonomous system topologies – An autonomous system (AS) is a collection of routers that are under common administrative control, and that share the same routing characteristics. When a group of autonomous systems share routing information, they are commonly referred to as a confederation of autonomous systems. (RFC1930 and RFC975 address these concepts in much greater detail). In simple terms, an AS is a logical distinction that encompasses physical network elements based on the commonness of their configurations.

With regard to RIP and OSPF, RIP autonomous systems cannot be segmented, and all routing information must be advertised (broadcast) through the entire AS. This can become difficult to manage and can result in excessive routing information traffic. OSPF, on the other hand, employs the concept of Areas, and allows for logically, manageable segmentation to control the sharing of information within an AS. OSPF areas begin with the backbone area (area 0 or 0.0.0.0), and all other areas must connect to this backbone area (although there are exceptions). This ability to segment the routing AS helps to ensure that it never becomes too large to manage, or too computationally intensive for the routers to handle.

## OSPF Terms

OSPF is substantially more complicated to configure and maintain than RIP. The following concepts are critical to understanding an OSPF routing environment:

- Link state – As it pertains to OSPF, a link is an egress interface on a router, and the state describes characteristics of that interface, such as its cost. Link states are sent in the form of Link State Advertisements (*LSA*) which are contained within Link State Update (*LSU*) packets, one of five types of OSPF packets.
- Cost – A quantification of the overhead required to send a packet along a particular link. Cost is calculated by dividing a reference bandwidth (usually 100mbit, or  $10^8$  bit) by an interface's speed. The lower the cost, the more preferable the link. Some common path costs:

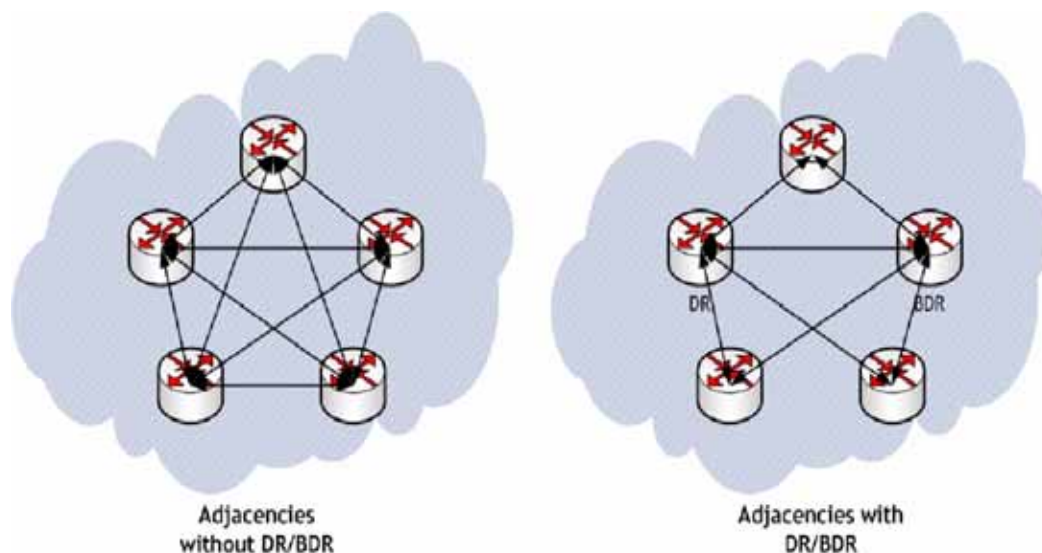
Interface	Divided by $10^8$ (100mbit) = OSPF Cost
Fast Ethernet	1
Ethernet	10
T1 (1.544mbit)	64
DSL (1mbit)	100
DSL (512kbps)	200
64kbps	1562
56kbps	1785

- Area – The network comprising the group of OSPF routers intended to share a common Link State Database. OSPF networks are built around the backbone area (area 0, or 0.0.0.0) and all other areas must connect to the backbone area (unless virtual links are

used, which is generally discouraged). Area assignment is interface specific on an OSPF router; in other words, a router with multiple interfaces can have those interfaces configured for the same or different areas.

- Neighbors – OSPF routers on a common network segment have the potential to become neighbors by means of sending Hello packets. Hello packets act as a form of advertisement and identification, and if two OSPF routers share a common set of certain characteristics, they will become neighbors upon seeing their own router ID in the other router's Hello packet. Hello packets are also used in the *DR* (Designated Router) and *BDR* (Backup Designated Router) election process. For two routers to become neighbors, the characteristics that they must have in common are:
  - Area-ID – An area ID identifies an OSPF *area* with a 32 bit value, and is generally represented in an IP address format. OSPF requires at a minimum the backbone area, area 0 (or 0.0.0.0) for operation.
  - Authentication – Authentication types can generally be set to none, simple text, or MD5. When using simple text, it should only be used for identification purposes, since it is sent in the clear. For security, MD5 should be used.
  - Timer intervals – 'Hello' and 'Dead' intervals must be the same. The Hello interval specifies the number of seconds between Hello packets (as a Keepalive function), and the Dead interval specifies the number of seconds after which a router will be considered unavailable if a Hello is not received.
  - Stub area flag – A *Stub area* is an area that only requires a single point of egress, and therefore does not require a full list of external link advertisements. The stub area flag on two potential neighbors must be the same to avoid inappropriate link state exchanges. Another factor that affects neighboring is the kind of network. OSPF recognizes three network types:
    - Broadcast – For example, Ethernet. In broadcast networks, neighboring can be established with all other routers in the broadcast domain.
    - Point to Point – For example, serial links. In point to point (or point to multipoint) networks, neighboring can be established with the router at the other end of the link.
    - NBMA (non-broadcast multiple access) – For example, frame relay. In NBMA networks, neighbors must be explicitly declared.
- Link State Database – The Link State Database is composed of the LSA's sent and received by *neighboring* OSPF routers that have created *adjacencies* within an *area*. The database, once complete, will contain all the link state information for a given area, at which time the Shortest Path First (SPF) algorithm will be applied to determine the optimal route to all connected networks based on cost. The SPF algorithm employs the Dijkstra pathfinding algorithm, which essentially regards all routers as vertices in a graph, and computes the cost between each vertex.
- Adjacencies – OSPF routers exchange LSA's with adjacent routers to create the LSDB. Adjacencies are created in different fashions depending on the network type (see Neighbors section above). Generally, the network type is broadcast (e.g. Ethernet) so adjacencies are formed by the exchanging OSPF packets in a handshake-like fashion (see OSPF Packet types below). To minimize the amount of information exchanged between adjacent routers, segments (broadcast domains) with multiple OSPF routers elect a Designated Router (DR) and a Backup Designated Router (BDR) using Hello packets.
- DR (Designated Router) – On multi-access segments, OSPF routers elect a DR and a BDR, and all other routers on the segment create adjacencies with the DR and the BDR. DR election is based on a router's OSPF Priority, which is a configurable value from 0 (not eligible for DR) to 255. The router with the highest priority becomes the DR. In the event of a priority tie, the router with the highest Router ID (based on interface addressing) wins. Once a router is the DR, its role is uncontested, until it becomes unavailable.

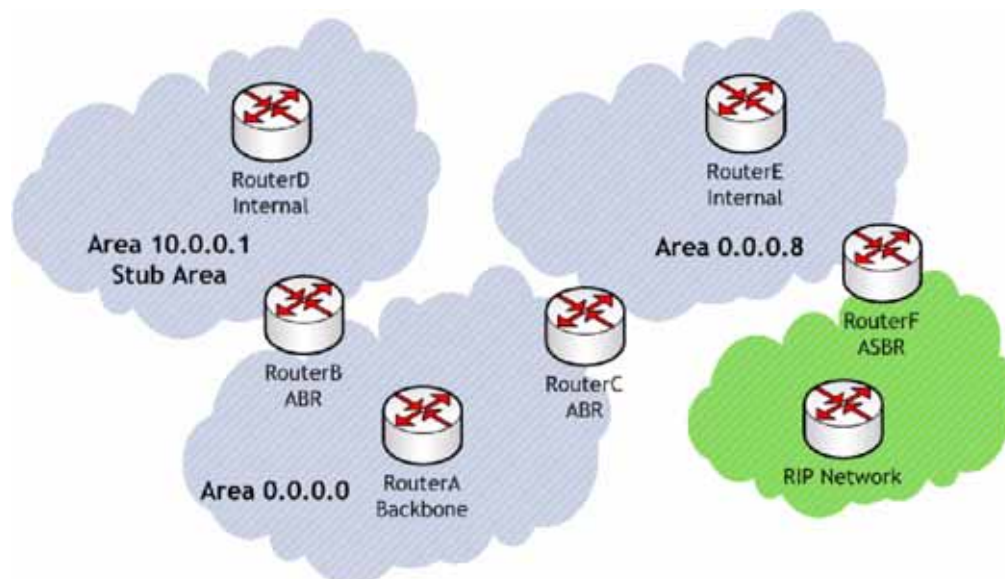
LSA's are then exchanged within LSU's across these adjacencies rather than between each possible pairing combination of routers on the segment. Link state updates are sent by non-DR routers to the multicast address 224.0.0.6, the RFC1583 assigned 'OSPF Designated Routers' address. They are also flooded by DR routers to the multicast address 224.0.0.5 'OSPF All Routers' for all routers to receive the LSA's.



- OSPF Packet types – The five types of OSPF packets are:
  - Hello (OSPF type 1) – Sent at a certain interval to establish and maintain relationships with neighboring OSPF routers, and elect Designated Routers. (*Sent during the initialization and the 2-WAY phases on LSDB synchronization*).
  - Database Description (OSPF type 2) – Sent between OSPF routers during the creation of an adjacency. *During the Exstart phase of LSDB synchronization*, DD packets establish an ISN (initial sequence number) used to track LSA's, and they establish a master/slave relationship between neighboring OSPF routers. *In the Exchange phase of LSDB synchronization*, they contain short versions of Link State Advertisements. Because DD exchanges can span multiple packets, they are exchanged in a poll (master) and response (slave) fashion to ensure completeness.
  - Link State Request (OSPF type 3) – *During the Loading phase of LSDB synchronization*, LSR packets are sent to request database updates from a neighbor. This is the final step in the establishment of an adjacency.
  - Link State Update (OSPF type 4) – Sent in response to Link State Requests, LSU packets flood adjacencies with Link State Advertisements to achieve LSDB synchronization.
  - Link State Acknowledgement (OSPF type 5) – To ensure reliability of LSA flooding, all updates are acknowledged.
- Link State Advertisements (LSA) – There are 7 types of LSA's:
  - Type 1 (Router Link Advertisements) - Sent by an OSPF router to describe the links to each area to which it belongs. Type 1 LSA's are only flooded into a router's area.
  - Type 2 (Network Links Advertisements) – Sent by the DR for an area describing the set of routers within the network. Type 2 LSA's are only flooded into a router's area.
  - Type 3 (Summary Link Advertisements) – Sent across areas by ABR's (Area Border Routers) to describe the networks within an area. Type 3 LSA's are also used for route aggregation purposes, and are not sent to Totally Stubby Areas.

- Type 4 (AS Summary Link Advertisements) – Sent across areas by ABR's to describe networks within a different AS. Type 4 LSA's are not sent to Stub Areas.
  - Type 5 (AS External Link Advertisements) – Sent by ASBR (Autonomous System Boundary Routers) to describe routes to networks in a different AS. Type 5 LSA's are not sent to Stub Areas. There are two types of External Link Advertisements:
    - External Type 1 - Type 1 packets add the internal link cost to the external link cost when calculating a link's metric. A Type 1 route is always preferred over a Type 2 route to the same destination.
    - External Type 2 - Type 2 packets only use the external link cost to determine the metric. Type 2 is generally used when there is only one path to an external AS.
  - Type 6 (Multicast OSPF) - Spooky. See RFC1584.
  - Type 7 (NSSA AS External Link Advertisements) – Sent by ASBR's that are part of an NSSA (see 'Stub Area').
- Stub Area – A stub area is an area that only requires one path, rather than an optimal path. This can be an area with only a single point of egress, or it can be an area where SPF optimization is not necessary. All routers in a stub area must be configured as stub routers, and rather than receiving the full state database, and computing the SPF tree, they will receive only a summary link information. There are different type of stub area:
    - Stub area – The standard stub area receives all LSA's except for LSA type 5 (AS External Link advertisement). This helps to keep the LSDB smaller, and reduces the computational overhead on the router.
    - Totally Stubby Area – A special type of stub area into which LSA types 3 (Summary Links), 4 (AS Summary Links) and 5 are not passed. Only intra-area routes, and a default route are advertised into totally stubby areas.
    - NSSA (Not So Stubby Area) – Described by RFC3101, NSSA is a hybrid stub area that allows external routes to be flooded within the NSSA area using type 7 LSA's (NSSA AS External Routes), but does not accept type 5 LSA's from other areas. NSSA's are useful when connecting a remote site running a different IGP (such as RIP) to an OSPF site, where the remote site's routes do not need to be distributed back to the main OSPF site. An NSSA ABR (Area Border Router) also has the ability to translate type 7 to type 5 LSA's (this is possible only from the SonicOS Enhanced CLI).

- Router Types – OSPF recognizes 4 types of routers, based on their roles:



- IR (Internal Router) - A router whose interfaces are all contained within the same area. An internal router's LSDB only contains information about its own area.
- ABR (Area Border Router) – A router with interfaces in multiple areas. An ABR maintains LSDB's for each area to which it is connected, one of which is typically the backbone.
- Backbone Router – A router with an interface connected to area 0, the backbone.
- ASBR (Autonomous System Boundary Router) – A router with an interface connected to a non-OSPF AS (such as a RIP network) which advertises external routing information from that AS into the OSPF AS.

## Configuring Advanced Routing Services



Note

ARS is a fully featured multi-protocol routing suite. The sheer number of configurable options and parameters provided is incongruous with the simplicity of a graphical user interface. Rather than limiting the functionality of ARS, an abbreviated representation of its capabilities has been rendered in the GUI, providing control over the most germane routing features, while the full command suite is available via the CLI. The ARS CLI can be accessed from an authenticated CLI session, and contains 3 modules:

- **route ars-nsm** – The Advanced Routing Services Network Services Module. This component provides control over core router functionality, such as interface bindings and redistributable routes.
- **route ars-rip** – The RIP module. Provides control over the RIP router.
- **route ars-ospf** – The OSPF module. Provides control over the OSPF router.

In general, all of the functionality needed to integrate the SonicWALL into most RIP and OSPF environments is available through the web-based GUI. The additional capabilities of the CLI will make more advanced configurations possible. Please refer to the appendix for the full set of ARS CLI commands.

By default, Advanced Routing Services are disabled, and must be enabled to be made available. At the top of the **Network > Routing** page, is a checkbox **Use Advanced Routing**. Toggling the state of this checkbox will require a reboot for the changes to take effect. When the SonicWALL is running in Advanced Routing mode, the top of the **Network > Routing** page will look as follows:

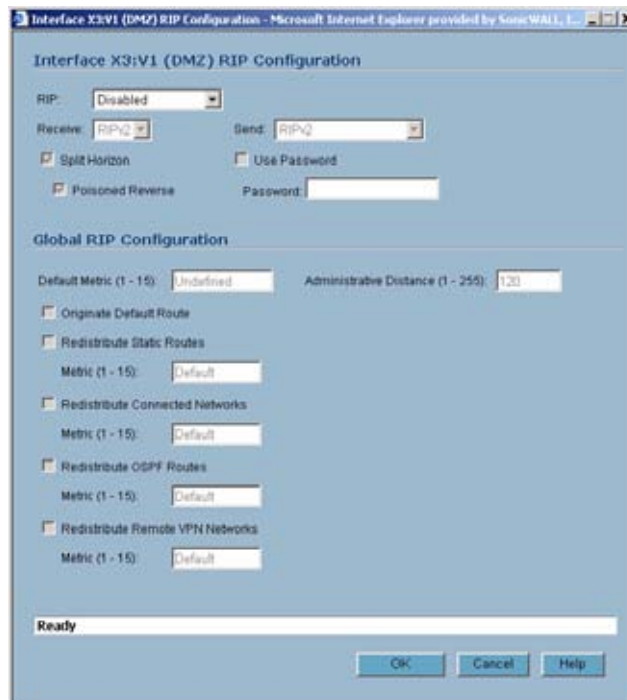
Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Disabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (N/A)	RIP Disabled		OSPF Disabled		
X3 (N/A)	RIP Disabled		OSPF Disabled		
X3:V1 (DMZ)	RIP Disabled		OSPF Disabled		
X4 (WLAN)	RIP Disabled		OSPF Disabled		
X5 (N/A)	RIP Disabled		OSPF Disabled		

The operation of the RIP and OSPF routing protocols is interface dependent. Each interface and virtual sub-interface can have RIP and OSPF settings configured separately, and each interface can run both RIP and OSPF routers.

Configure RIP and OSPF for default routes received from Advanced Routing protocols as follows:

## Configuring RIP

To configure RIP routing on an interface, select the (Configure) icon in the interface's row under the "Configure RIP" column. This will launch the **RIP Configuration** window.



## RIP Modes

- Disabled – RIP is disabled on this interface
- Send and Receive – The RIP router on this interface will send updates and process received updates.
- Send Only – The RIP router on this interface will only send updates, and will not process received updates. This is similar to the basic routing implementation.
- Receive Only – The RIP router on this interface will only process received updates.
- Passive – The RIP router on this interface will not process received updates, and will only send updates to neighboring RIP routers specified with the CLI 'neighbor' command. This mode should only be used when configuring advanced RIP options from the ars-rip CLI.

### Receive (Available in 'Send and Receive' and 'Receive Only' modes)

- RIPv1 – Receive only *broadcast* RIPv1 packets.
- RIPv2 – Receive only *multicast* RIPv2 packets. RIPv2 packets are sent by multicast, although some implementations of RIP routers (including basic routing on SonicWALL devices) have the ability to send RIPv2 in either broadcast or multicast formats.



#### Note

Be sure the device sending RIPv2 updates uses multicast mode, or the updates will not be processed by the ars-rip router.

### Send (Available in 'Send and Receive' and 'Send Only' modes)

- RIPv1 – Send *broadcast* RIPv1 packets.
- RIPv2 - v1 compatible – Send *multicast* RIPv2 packets that are compatible with RIPv1.
- RIPv2 – Send *multicast* RIPv2 packets.

*Split Horizon* – Enabling Split Horizon will suppress the inclusion of routes sent in updates to routers from which they were learned. This is a common RIP mechanism for preventing routing loops. See the 'maximum hops' entry at the start of Advanced Routing Services section.

*Poisoned Reverse* – Poison reverse is an optional mode of Split Horizon operation. Rather than suppressing the inclusion of learned routes, the routes are sent with a metric of infinity (16) thus indicating that they are unreachable. See the 'maximum hops' entry at the start of Advanced Routing Services section.

*Use Password* – Enables the use of a plain-text password on this interface, up to 16 alphanumeric characters long, for identification.

*Default Metric* – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, OSPF, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 15.

*Administrative Distance* – The administrative distance value is used by routers in selecting a path when there is more than one route to a destination, with the smaller distance being preferred. The default value is 120, minimum is 1, and maximum is 255.

*Originate Default Route* – This checkbox enables or disables the advertising of the SonicWALL's default route into the RIP system.

*Redistribute Static Routes* – Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

*Redistribute Connected Networks* - Enables or disables the advertising of locally connected networks into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

*Redistribute OSPF Routes* - Enables or disables the advertising of routes learned via OSPF into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

*Redistribute Remote VPN Networks* - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system. The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the 'Default Metric' setting.

Routes learned via RIP will appear in the Route Policies table as 'OSPR or RIP routes':

<input type="checkbox"/> 4	Any	66.182.95.84/27	Any	10.50.165.1	X2	120	4	<b>Comment</b>	
<input type="checkbox"/> 5	Any	LAN Primary Subnet	Any	0.0.0.0	XX			OSPF or RIP Route	

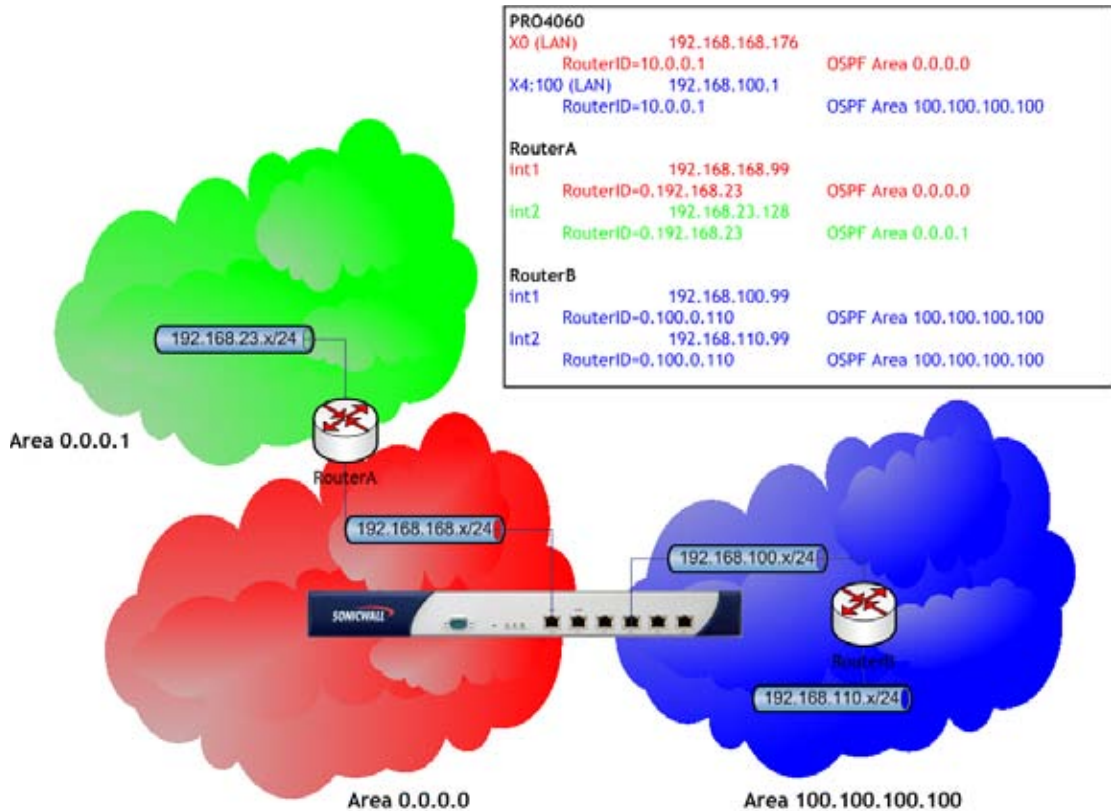
## Configuring OSPF



**Note**


OSPF design concepts are beyond the scope of this document. The following section describes how to configure a SonicWALL to integrate into an OSPF network, be it existing or newly implemented, but it does not offer design guidelines. For terms used throughout this section, refer to the 'OSPF Terms' section above.

Consider the following simple example network:





The diagram illustrates an OSPF network where the backbone (area 0.0.0.0) comprises the X0 interface on the SonicWALL and the int1 interface on Router A. Two additional areas, 0.0.0.1 and 100.100.100.100 are connected, respectively, to the backbone via interface int2 on ABR Router A, and via the X4:100 VLAN sub-interface on the SonicWALL.

To configure OSPF routing on the X0 and the X4:100 interfaces, select the  (Configure) icon in the interface's row under the "Configure OSPF" column. This will launch the following window:

## OSPFv2 Setting

- Disabled – OSPF Router is disabled on this interface
- Enabled – OSPF Router is enabled on this interface
- Passive – The OSPF router is enabled on this interface, but only advertises connected networks using type 1 LSA's (Router Link Advertisements) into the local area. This is different from the 'Redistribute Connected Networks' options, which would cause the OSPF router to behave as an ASBR, and to use type 5 LSA's (AS External Link Advertisement) to flood the advertisements into all non-stub areas. See the 'OSPF Terms' section for more information.

**Dead Interval** – The period after with an entry in the LSDB is removed if not Hello is received. The default is 40 seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

**Hello Interval** – The period of time between Hello packets. The default is 10 seconds, with a minimum of 1 and a maximum on 65,535. Be sure this value agrees with the other OSPF routers on the segment for successful neighbor establishment.

**Authentication** - Be sure this setting agrees with the other OSPF routers on the segment for successful neighbor establishment.

- Disabled – No authentication is used on this interface.
- Simple Password – A plain-text password is used for identification purposes by the OSPF router on this interface.

- Message Digest – An MD5 hash is used to securely identify the OSPF router on this interface.

*OSPF Area* – The OSPF Area can be represented in either IP or decimal notation. For example, you may represent the area connected to X4:100 as either 100.100.100.100 or 1684300900.

*OSPFv2 Area Type* – See the ‘OSPF Terms’ section above for a more detailed description of these settings.

- Normal – Receives and sends all applicable LSA types.
- Stub Area – Does not receive type 5 LSA’s (AS External Link Advertisements)
- Totally Stubby Area – Does not receive LSA types 3, 4, or 5.
- Not So Stubby Area – Receives type 7 LSA’s (NSSA AS External Routes).

*Interface Cost* – Specifies the overhead of sending packets across this interface. The default value is 10, generally used to indicate an Ethernet interface. The minimum value is 1 (e.g. Fast Ethernet) and the maximum value is 65,535 (e.g. pudding).

*Router Priority* – The router priority value is used in determining the Designated Router (DR) for a segment. The higher the value, the higher the priority. In the event of a priority tie, the Router ID will act as the tie-breaker. Setting a value of 0 makes the OSPF router on this interface ineligible for DR status. The default value is 1, and the maximum value is 255.

*OSPF Router ID* – The Router ID can be any value, represented in IP address notation. It is unrelated to any of the IP addresses on the SonicWALL, and can be set to any *unique* value within your OSPF network.

*ABR Type* – Allows for the specification of the topology with which this OSPF router will be participating, for the sake of compatibility. The options are:

- Standard – Full RFC2328 compliant ABR OSPF operation.
- Cisco – For interoperating with Cisco’s ABR behavior, which expects the backbone to be configured and active before setting the ABR flag.
- IBM – For interoperating with IBM’s ABR behavior, which expects the backbone to be configured before settings the ABR flag.
- Shortcut – A ‘shortcut area’ enables traffic to go through the non-backbone area with a lower metric whether or not the ABR router is attached to area 0.

*Default Metric* – Used to specify the metric that will be used when redistributing routes from other (Default, Static, Connected, RIP, or VPN) routing information sources. The default value (undefined) is 1 and the maximum is 16,777,214.

*Originate Default Route* – Controls the advertising of the SonicWALL security appliance’s default route into the OSPF system on this interface. The options are:

- Never – Disables advertisement of the default route into the OSPF system.
- When WAN is up – Advertises the default route into the OSPF system when the WAN is online. The default route is always advertised as an External Type 2 using LSA Type 5.
- Always – Enables advertisement of the default route into the OSPF system. The default route is always advertised as an External Type 2 using LSA Type 5.



**Note**

The following applies to all Redistributed routes: The metric can be explicitly set for this redistribution, or it can use the value (default) specified in the ‘Default Metric’ setting. An optional route tag value can be added to help other routers identify this redistributed route (the default tag value is 0). The redistributed route advertisement will be an LSA Type 5, and the type may be selected as either Type 1 (adds the internal link cost) or Type 2 (only uses the external link cost).

*Redistribute Static Routes* – Enables or disables the advertising of static (Policy Based Routing) routes into the OSPF system.

*Redistribute Connected Networks* - Enables or disables the advertising of locally connected networks into the OSPF system.

*Redistribute RIP Routes* - Enables or disables the advertising of routes learned via RIP into the OSPF system.

*Redistribute Remote VPN Networks* - Enables or disables the advertising of static (Policy Based Routing) routes into the RIP system.

The Routing Protocols section will show the status of all active OSPF routers by interface:

Interface (Zone)	RIP	Configure RIP	OSPFv2	Configure OSPF	OSPF Neighbor Status
X0 (LAN)	RIP Disabled		OSPF Enabled		
X1 (WAN)	RIP Disabled		OSPF Disabled		
X2 (WLAN)	RIP Disabled		OSPF Disabled		
X3 (LAN)	RIP Disabled		OSPF Disabled		
X4 (WAN)	RIP Disabled		OSPF Disabled		
▶ X4V100 (LAN)	RIP Disabled		OSPF Enabled		
▶ X4V150 (Sales)	RIP Disabled		OSPF Disabled		
▶ X4V250 (Engineering)	RIP Disabled		OSPF Disabled		
X5 (WAN)	RIP Disabled		OSPF Disabled		

The and Status LED's indicate whether or not there are active neighbors, and can be clicked on for more detail:

Router-ID	Current State	Priority	IP Address
0.192.168.23	Full / DR	1	192.168.168.99

The Routing Policies section will show routes learned by OSPF as 'OSPF or RIP Routes':

#	Source	Destination	Service	Gateway	Interface	Metric	Priority	Comment	Configure
1	Any	192.168.110.0/24	Any	192.168.100.99		110	11		
2	Any	192.168.23.0/24	Any	192.168.168.99	X1	110	10		
3	Any	WAN Primary Subnet	Any	0.0.0.0	X1			OSPF or RIP Route	





## CHAPTER 21

# Configuring NAT Policies

---

## Network > NAT Policies

- [“NAT Policies Table” on page 246](#)
- [“NAT Policy Settings Explained” on page 248](#)
- [“NAT Policies Q&A” on page 249](#)

The Network Address Translation (NAT) engine in SonicOS Enhanced allows users to define granular NAT policies for their incoming and outgoing traffic. By default, the SonicWALL security appliance has a preconfigured NAT policy to allow all systems connected to the **LAN** interface to perform

many-to-one NAT using the IP address of the **WAN** interface, and a policy to not perform NAT when traffic crosses between the other interfaces. This chapter explains how to set up the most common NAT policies.

Understanding how to use NAT policies starts with an the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester’s IP address, the protocol information of the requestor, and the destination’s IP address. The NAT Policies engine in SonicOS Enhanced can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

You can add up to 512 NAT Policies on a SonicWALL security appliance running SonicOS Enhanced, and they can be as granular as you need. It’s also possible to create multiple NAT policies for the same object – for instance, you can specify that an internal server use one IP address when accessing Telnet servers, and to use a totally different IP address for all other protocols. Because the NAT engine in SonicOS Enhanced supports inbound port forwarding, it is possible to hide multiple internal servers off the WAN IP address of the SonicWALL security appliance. The more granular the NAT Policy, the more precedence it takes.

# NAT Policies Table

The NAT Policies table allows you to view your NAT Policies by **Custom Policies**, **Default Policies**, or **All Policies**.

Network > NAT Policies Public Server Wizard... Clear Statistics ?

NAT Policies Items 1 to 17 (of 17)

View Style:  All Policies  Custom Policies  Default Policies

#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound				
<input checked="" type="checkbox"/> 1	Any	Original	X3-V100 IP	Original	HTTPS Management	Original	X3-V100	X3-V100	1		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 2	Any	Original	X3-V100 IP	Original	HTTP Management	Original	X3-V100	X3-V100	2		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 3	All Interface IP	X1 IP	Any	Original	Any	Original	Any	X1	3		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 4	Any	Original	X3-V20 IP	Original	HTTPS Management	Original	X3-V20	X3-V20	4		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 5	Any	Original	X3-V20 IP	Original	HTTP Management	Original	X3-V20	X3-V20	5		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 6	Any	Original	X4 IP	Original	HTTPS Management	Original	X4	X4	6		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 7	Any	Original	X4 IP	Original	HTTP Management	Original	X4	X4	7		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 8	Any	Original	X1 IP	Original	HTTPS Management	Original	X1	X1	8		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 9	Any	Original	X1 IP	Original	HTTP Management	Original	X1	X1	9		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 10	Any	Original	X0 IP	Original	Ping	Original	X0	X0	10		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 11	Any	Original	X0 IP	Original	HTTPS Management	Original	X0	X0	11		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 12	Any	Original	X0 IP	Original	HTTP Management	Original	X0	X0	12		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 13	Any	X1 IP	Any	Original	Any	Original	X3-V100	X1	13		<input type="checkbox"/>	
<input type="checkbox"/> 14	Any	X1 IP	Any	Original	Any	Original	X3-V20	X1	14		<input type="checkbox"/>	
<input type="checkbox"/> 15	Any	X1 IP	Any	Original	Any	Original	X4	X1	15		<input type="checkbox"/>	
<input type="checkbox"/> 16	Any	X1 IP	Any	Original	Any	Original	X0	X1	16		<input type="checkbox"/>	
<input checked="" type="checkbox"/> 17	Any	Original	Any	Original	Any	Original	Any	Any	17		<input checked="" type="checkbox"/>	

Add Delete Delete All

SONICWALL UNCOMPROMISED. EXTENDED SECURITY™

Network > NAT Policies Public Server Wizard... Clear Statistics ?

NAT Policies Items 1 to 24 (of 24)

View Style:  All Policies  Custom Policies  Default Policies

#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound				
<input checked="" type="checkbox"/> 1	WLAN Interface IP	Original	Any	Original	IKE	Original	Any	Any	1		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 2	Any	Original	WLAN Interface IP	Original	IKE	Original	Any	Any	2		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 3	WAN Interface IP	Original	Any	Original	IKE	Original	Any	Any	3		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 4	Any	Original	WAN Interface IP	Original	IKE	Original	Any	Any	4		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 5	Any	Original	OPT IP	Original	HTTPS Management	Original	OPT	OPT	5		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 6	Any	Original	OPT IP	Original	HTTP Management	Original	OPT	OPT	6		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 7	Any	Original	WAN Primary IP	Original	SMTP	Original	WAN	WAN	7		<input checked="" type="checkbox"/>	
<input checked="" type="checkbox"/> 8	Any	Original	WAN Primary IP	Original	Ping	Original	WAN	WAN	8		<input checked="" type="checkbox"/>	

System: Ready

**Tip**

Before configuring NAT Policies, be sure to create all Address Objects associated with the policy. For instance, if you are creating a One-to-One NAT policy, be sure you have Address Objects for your public and private IP addresses.

**Tip**

By default, LAN to WAN has a NAT policy predefined on the SonicWALL.

## Navigating and Sorting NAT Policy Entries

You can change the view your route policies in the **NAT Policies** table by selecting one of the view settings in the **View Style** menu. **All Policies** displays all the routing policies including **Custom Policies** and **Default Policies**. Initially, only the **Default Policies** are displayed in the **Route Policies** table when you select **All Policies** from the **View Style** menu.

The **NAT Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **Route Policies** table by using the navigation control bar located at the top right of the **Route Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed in the **#** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

Moving your pointer over the Comment icon in the **Configure** column of **NAT Policies** table displays the comments entered in the **Comments** field of the **Add NAT Policy** window.

Moving your pointer over the Statistics icon in the **Configure** column of **NAT Policies** table displays traffic statistics for the NAT policy.

Clicking the Delete icon (trashcan) deletes the NAT Policy entry. If the icon is dimmed, the NAT Policy is a default entry and you cannot delete it.

## NAT Policy Settings Explained

The following explains the settings used to create a NAT policy entry in the **Add NAT Policy** or **Edit NAT Policy** windows.



Click the **Add** button in the **Network > NAT Policies** page to display the **Add NAT Policy** window to create a new NAT policy or click the Edit icon in the **Configure** column for the NAT policy you want to edit to display the **Edit NAT Policy** window.

- **Original Source:** This drop-down menu setting is used to identify the Source IP address(es) in the packet crossing the SonicWALL security appliance, whether it's across interfaces, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects. These entries can be single host entries, address ranges, or IP subnets.
- **Translated Source:** This drop-down menu setting is what the SonicWALL security appliance translates the specified **Original Source** to as it exits the SonicWALL security appliance, whether it's to another interface, or into/out-of VPN tunnels. You can use the default Address Objects in SonicOS Enhanced, or you can create your own Address Objects entries. These entries can be single host entries, address ranges, or IP subnets.
- **Original Destination:** This drop-down menu setting is used to identify the Destination IP address(es) in the packet crossing the SonicWALL security appliance, whether it be across interfaces, or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Any** since the destination of the packet is not being changed, but the source is being changed. However, these Address Object entries can be single host entries, address ranges, or IP subnets.
- **Translated Destination:** This drop-down menu setting is what the SonicWALL translates the specified **Original Destination** to as it exits the SonicWALL security appliance, whether it's to another interface, or into/out-of VPN tunnels. When creating outbound NAT policies, this entry is usually set to **Original**, since the destination of the packet is not being changed, but the source is being changed. However, these Address Objects entries can be single host entries, address ranges, or IP subnets.
- **Original Service:** This drop-down menu setting is used to identify the IP service in the packet crossing the SonicWALL security appliance, whether it's across interfaces, or into/out-of VPN tunnels. You can use the default services on the SonicWALL, or you can create your own entries. For many NAT policies, this field is set to **Any**, as the policy is only altering source or destination IP addresses.



- **Translated Service:** This drop-down menu setting is what the SonicWALL security appliance translates the **Original Service** to as it exits the SonicWALL security appliance, whether it be to another interface, or into/out-of VPN tunnels. You can use the default services in the SonicWALL security appliance, or you can create your own entries. For many NAT Policies, this field is set to **Original**, as the policy is only altering source or destination IP addresses.
- **Inbound Interface:** This drop-down menu setting is used to specify the entry interface of the packet. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces.
- **Outbound Interface:** This drop-down is used to specify the exit interface of the packet once the NAT policy has been applied. This field is mainly used for specifying which WAN interface to apply the translation to. Of all fields in NAT policy, this one has the most potential for confusion. When dealing with VPNs, this is usually set to **Any**, since VPN tunnels aren't really interfaces. Also, as noted in the Quick Q&A' section of this chapter, when creating inbound 1-2-1 NAT Policies where the destination is being remapped from a public IP address to a private IP address, this field must be set to **Any**.
- **Comment:** This field can be used to describe your NAT policy entry. The field has a 32-character limit, and once saved, can be viewed in the main **Network > NAT Policies** page by running the mouse over the text balloon next to the NAT policy entry. Your comment appears in a pop-up window as long as the mouse is over the text balloon.
- **Enable NAT Policy:** By default, this box is checked, meaning the new NAT policy is activated the moment it is saved. To create a NAT policy entry but not activate it immediately, uncheck this box.
- **Create a reflective policy:** When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the **Add NAT Policy** window is automatically created.

## NAT Policies Q&A

### Why is it necessary to specify 'Any' as the destination interface for inbound 1-2-1 NAT policies?

It may seem counter-intuitive to do this, given that other types of NAT policies require you to specify the destination interface, but for this type of NAT policy, this is what is necessary. The SonicWALL security appliance uses this field during the NAT Policy lookup and validates it against the packet that it receives, but if this is set to some internal interface such as LAN, the lookup fails because at that point, the SonicWALL security appliance does not know that the packet is going to LAN. It's not until after the SonicWALL security appliance performs the NAT Policy lookup that it knows that the packet is going to LAN. At the precise time that the SonicWALL security appliance does the NAT Policy lookup, the packet looks like it is going from WAN -> WAN (or whatever interface it is coming in on), since doing a route lookup on the NAT Public address returns the Public interface.

### Can I manually order the NAT Policies?

No, the SonicWALL security appliance automatically orders them, depending on the granularity of the rule. This means that you can create NAT policy entries for the same objects, if each policy has more granularity than the existing policy. For example, you can create a NAT policy

to translate all LAN systems to the WAN IP Address, then create a policy saying that a specific system on that LAN use a different IP address, and additionally, create a policy saying that specific use another IP address when using HTTP.

## Can I have multiple NAT policies for the same objects?

Yes – please read the section above.

## What are the NAT ‘System Polices’?

On the **Network > NAT Policies** page, notice a radio button labeled **System Polices**. If you choose this radio button, the NAT Policies page displays all of the default, auto-created NAT policies for the SonicWALL security appliance. These policies are default settings for the SonicWALL security appliance to operate properly, and cannot be deleted. For this reason, they are listed in their own section, in order to make the user-created NAT policies easier to browse. If you wish to see user-created NAT policies along with the default NAT policies, simply check the radio button next to ‘All Policies’.

## Can I write NAT policies for VPN traffic?

Yes, this is possible if both sides of the VPN tunnel are SonicWALL security policies running SonicOS Enhanced firmware. Please refer to the technote **SonicOS Enhanced NAT VPN Overlap** for instructions on how to perform NAT on traffic entering and exiting VPN tunnels. Available at <http://www.sonicwall.com/us/Support.html>.

## Why do I have to write two policies for 1-2-1 traffic?

With the new NAT engine, it’s necessary to write two policies – one to allow incoming requests to the destination public IP address to reach the destination private IP address (uninitiated inbound), and one to allow the source private IP address to be remapped to the source public IP address (initiated outbound). It takes a bit more work, but it’s a lot more flexible.

## NAT Load Balancing Overview

This section provides an introduction to the NAT Load Balancing feature. It contains the following subsections:

- [“NAT LB Mechanisms” on page 251](#)
- [“Which NAT LB Method Should I Use?” on page 252](#)
- [“Caveats” on page 252](#)
- [“Details of Load Balancing Algorithms” on page 253](#)

Network Address Translation (NAT) & Load Balancing (LB) provides the ability to balance incoming traffic across multiple, similar network resources. Do not confuse this with the WAN ISP & LB feature on the SonicWALL appliance. While both features can be used in conjunction, WAN ISP & LB is used to balance outgoing traffic across two ISP connections, and NAT LB is primarily used to balance incoming traffic.

Load Balancing distributes traffic among similar network resources so that no single server becomes overwhelmed, allowing for reliability and redundancy. If one server becomes unavailable, traffic is routed to available resources, providing maximum uptime.

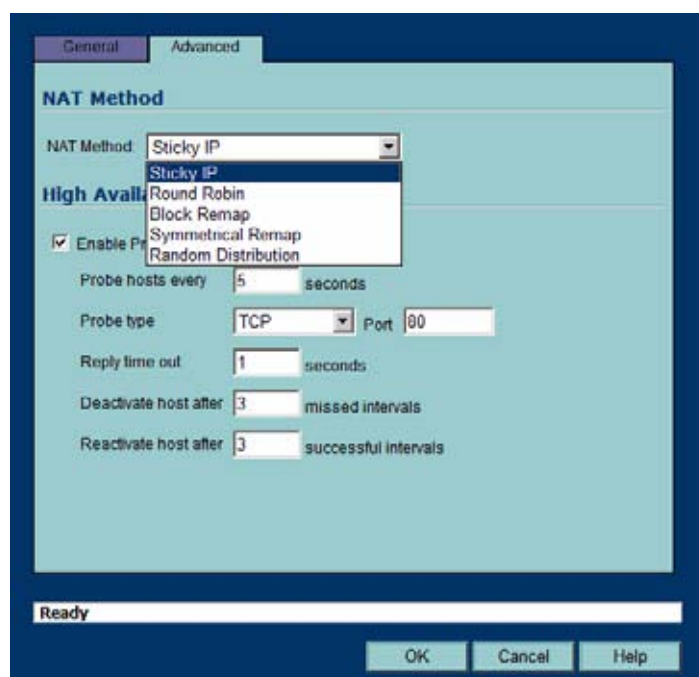
This document details how to configure the necessary NAT, load balancing, health check, logging, and firewall rules to allow systems from the public Internet to access a Virtual IP (VIP) that maps to one or more internal systems, such as Web servers, FTP servers, or SonicWALL SSL-VPN appliances. This Virtual IP may be independent of the SonicWALL appliance or it may be shared, assuming the SonicWALL appliance itself is not using the port(s) in question.

The examples in this document use two SonicWALL PRO 4100 appliances in high-availability mode, two generic Web servers, and two SonicWALL SSL-VPN 2000 appliances. Please note that it is not necessary to have two appliances to perform NAT/LB – it is just another layer of protection that can be easily added to your environment to assure uptime to critical internal resources that have high uptime requirements (typically a driving factor in load balancing systems in the first place).

Please note that the load balancing capability in SonicOS Enhanced 4.0, while fairly basic, will satisfy the requirements for many customer network deployments. Customers with environments needing more granular load balancing, persistence, and health-check mechanisms are advised to use a dedicated third-party load balancing appliance (prices run from US\$4,000 to US\$25,000 per device).

## NAT LB Mechanisms

NAT load balancing is configured on the **Advanced** tab of a NAT policy.



### Note

This tab can only be activated when a group is specified in one of the drop-down fields on the **General** tab of a NAT Policy. Otherwise, the NAT policy defaults to **Sticky IP** as the NAT method.

SonicOS offers the following NAT methods:

- **Sticky IP** – Source IP always connects to the same Destination IP (assuming it is alive). This method is best for publicly hosted sites requiring connection persistence, such as Web applications, Web forms, or shopping cart applications. This is the default mechanism, and is recommended for most deployments.

- **Round Robin** – Source IP cycles through each live load-balanced resource for each connection. This method is best for equal load distribution when persistence is not required.
- **Block Remap/Symmetrical Remap** – These two methods are useful when you know the source IP addresses/networks (e.g. when you want to precisely control how traffic from one subnet is translated to another).
- **Random Distribution** – Source IP connects to Destination IP randomly. This method is useful when you wish to randomly spread traffic across internal resources.
- **NAT Method** – This drop-down allows the user to specify one of five load balancing methods: Sticky IP, Round Robin, Block Remap, Symmetric Remap, or Random Distribution. For most purposes, Sticky IP is preferred.
- **Enable Probing** – When checked, the SonicWALL will use one of two methods to probe the addresses in the load-balancing group, using either a simple ICMP ping query to determine if the resource is alive, or a TCP socket open query to determine if the resource is alive. Per the configurable intervals, the SonicWALL can direct traffic away from a non-responding resource, and return traffic to the resource once it has begun to respond again.

## Which NAT LB Method Should I Use?

Requirement	Deployment Example	NAT LB Method
Distribute load on server equally without need for persistence	External/ Internal servers (i.e. Web, FTP, etc.)	Round Robin
Indiscriminate load balancing without need for persistence	External/ Internal servers (i.e. Web, FTP, etc.)	Random Distribution
Requires persistence of client connection	E-commerce site, Email Security, SSL-VPN appliance  (Any publicly accessible servers requiring persistence)	Sticky IP
Precise control of remap of source network to a destination range	LAN to DMZ Servers  E-mail Security, SSL-VPN	Block Remap
Precise control of remap of source network and destination network	Internal Servers (i.e. Intranets or Extranets)	Symmetrical Remap

## Caveats

- The NAT Load Balancing Feature is only available in SonicOS Enhanced 4.0 and newer.
- Only two health-check mechanisms at present (ICMP ping and TCP socket open).
- No higher-layer persistence mechanisms at present (Sticky IP only).
- No “sorry-server” mechanism at present if all servers in group are not responding.
- No “round robin with persistence” mechanism at present.
- No “weighted round robin” mechanism at present.
- No method for detecting if resource is strained, at present.
- While there is no limit to the number of internal resources the SonicWALL appliance can load-balance to, and there no limit to the number of hosts it can monitor, abnormally large load-balancing groups (25+resources) may impact performance.

## Details of Load Balancing Algorithms

This appendix describes how the SonicWALL security appliance applies the load balancing algorithms:

- **Round Robin** - Source IP connects to Destination IP alternately
- **Random Distribution** - Source IP connects to Destination IP randomly
- **Sticky IP** - Source IP connects to same Destination IP
- **Block Remap** - Source network is divided by size of the Destination pool to create logical segments
- **Symmetrical Remap** - Source IP maps to Destination IP (for example, 10.1.1.10 -> 192.168.60.10.)

### Sticky IP Algorithm

Source IP is modulo with the size of the server cluster to determine the server to remap it to. The following two examples show how the Sticky IP algorithm works.

Example one:  
 192.168.0.2 to 192.168.0.4  
 Translated Dest = 10.50.165.0/30 (Network)

Packet Src IP = 192.168.0.2  
 192.168.0.2 = C0A80002 = 3232235522 = 110000001010100000000000000010

IP → Hex → Dec → Binary

**Sticky IP Formula** = Packet Src IP=3232235522 [modulo] TransDest Size=2  
 = 3232235522 [modulo] 2  
 = 0  
 2 divides into numerator evenly. There is no remainder thus 0  
**Sticky IP Formula yields offset of 0**  
**Destination remapping to 10.50.165.1**

Example two:  
 192.168.0.2 to 192.168.0.4  
 Translated Dest = 10.50.165.1 - 10.50.165.3 (Range)

Packet Src IP = 192.168.0.2  
 192.168.0.2 = C0A80002 = 3232235522 = 110000001010100000000000000010

IP → Hex → Dec → Binary

**Sticky IP Formula** = Packet Src IP=3232235522 [modulo] TransDest Size=3  
 = 3232235522 [modulo] 3  
 = 1077411840.6666667 - 1077411840  
 = 0.6666667 X 3  
 = 2  
**Sticky IP Formula yields offset of 2**  
**Destination remapping to 10.50.165.3**

## Creating NAT Policies

NAT policies allow you the flexibility to control Network Address Translation based on matching combinations of Source IP address, Destination IP address, and Destination Services. Policy-based NAT allows you to deploy different types of NAT simultaneously. This section contains the following subsections:

- [“Creating a Many-to-One NAT Policy” on page 254](#)
- [“Creating a Many-to-Many NAT Policy” on page 255](#)
- [“Creating a One-to-One NAT Policy for Outbound Traffic” on page 256](#)
- [“Creating a One-to-One NAT Policy for Inbound Traffic \(Reflective\)” on page 257](#)
- [“Configuring One-to-Many NAT Load Balancing” on page 257](#)
- [“Inbound Port Address Translation via One-to-One NAT Policy” on page 259](#)
- [“Inbound Port Address Translation via WAN IP Address” on page 260](#)
- [“Using NAT Load Balancing” on page 263](#)

For this chapter, the examples use the following IP addresses as examples to demonstrate the NAT policy creation and activation. You can use these examples to create NAT policies for your network, substituting your IP addresses for the examples shown here:

- 192.168.10.0/24 IP subnet on interface **LAN**
- 67.115.118.64/27 IP subnet on interface **WAN**
- 192.168.30.0/24 IP subnet on interface **Opt**
- **LAN** IP address is 192.168.10.1
- **WAN** IP address is 67.115.118.68
- **Opt** ‘Sales’ IP address is 192.168.30.1
- Webserver’s “private” address at 192.168.30.200
- Webserver’s “public” address at 67.115.118.70
- Public IP range addresses of 67.115.118.71 – 67.115.118.74

### Creating a Many-to-One NAT Policy

Many-to-One is the most common NAT policy on a SonicWALL security appliance, and allows you to translate a group of addresses into a single address. Most of the time, this means that you’re taking an internal “private” IP subnet and translating all outgoing requests into the IP address of the SonicWALL security appliance WAN port, such that the destination sees the request as coming from the IP address of the SonicWALL security appliance WAN port, and not from the internal private IP address.

This policy is easy to set up and activate. From the Management Interface, go to the **Network > NAT Policies** page and click on the **Add** button. The **Add NAT Policy** window is displayed for adding the policy. To create a NAT policy to allow all systems on the **Opt** interface to initiate traffic using the SonicWALL security appliance’s WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** Opt Subnet
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original

- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. This policy can be duplicated for subnets behind the other interfaces of the SonicWALL security appliance – just replace the **Original Source** with the subnet behind that interface, adjust the source interface, and add another NAT policy.

## Creating a Many-to-Many NAT Policy

The Many-to-Many NAT policy allows you to translate a group of addresses into a group of different addresses. This allows the SonicWALL security appliance to utilize several addresses to perform the dynamic translation. Thus allowing a much higher number of concurrent the SonicWALL security appliance to perform up to a half-million concurrent connections across the interfaces.

This policy is easy to set up and activate. You first need to go to the **Network > Address Objects** and click on the **Add** button at the bottom of the screen. When the **Add Address Object** window appears, enter in a description for the range in the **Name** field, choose **Range** from the drop-down menu, enter the range of addresses (usually public IP addresses supplied by your ISP) in the **Starting IP Address** and **Ending IP Address** fields, and select **WAN** as the zone from the **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Select **Network > NAT Policies** and click on the **Add** button. The Add NAT Policy window is displayed. To create a NAT policy to allow the systems on the LAN interface to initiate traffic using the public range addresses, choose the following from the drop-down menus:

- **Original Source:** LAN Primary Subnet
- **Translated Source:** public\_range
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** LAN
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance dynamically maps outgoing traffic using the four available IP addresses in the range we created.

You can test the dynamic mapping by installing several systems on the LAN interface at a spread-out range of addresses (for example, 192.168.10.10, 192.168.10.100, and 192.168.10.200) and accessing the public website <http://www.whatismyip.com> from each system. Each system should display a different IP address from the range we created and attached to the NAT policy.

## Creating a One-to-One NAT Policy for Outbound Traffic

One-to-One NAT for outbound traffic is another common NAT policy on a SonicWALL security appliance for translating an internal IP address into a unique IP address. This is useful when you need specific systems, such as servers, to use a specific IP address when they initiate traffic to other destinations. Most of the time, a NAT policy such as this one-to-one NAT policy for outbound traffic is used to map a server's private IP address to a public IP address, and it's paired with a reflective (mirror) policy that allows any system from the public Internet to access the server, along with a matching firewall access rule that permits this. Reflective NAT policies are covered in the next section.

This policy is easy to set up and activate. Select **Network > Address Objects** and click on the **Add** button at the bottom of the screen. In the **Add Address Object** window, enter a description for server's private IP address in the **Name** field. Choose **Host** from the **Type** menu, enter the server's private IP address in the **IP Address** field, and select the zone that the server assigned from the **Zone Assignment** menu. Click **OK**. Then, create another object in the **Add Address Object** window for the server's public IP address and with the correct values, and select **WAN** from **Zone Assignment** menu. When done, click on the **OK** button to create the range object.

Next, select **Network > NAT Policies** and click on the **Add** button to display the **Add NAT Policy** window. To create a NAT policy to allow the webserver to initiate traffic to the public Internet using its mapped public IP address, choose the following from the drop-down menus:

- **Original Source:** webserver\_private\_ip
- **Translated Source:** webserver\_public\_ip
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Checked

When done, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's private IP address to the public IP address when it initiates traffic out the WAN interface.

You can test the one-to-one mapping by opening up a web browser on the server and accessing the public website <http://www.whatismyip.com>. The website should display the public IP address we attached to the private IP address in the NAT policy we just created.



## Creating a One-to-One NAT Policy for Inbound Traffic (Reflective)

This is the mirror policy for the one created in the previous section when you check **Create a reflective policy**. It allows you to translate an external public IP addresses into an internal private IP address. This NAT policy, when paired with a 'permit' access policy, allows any source to connect to the internal server using the public IP address; the SonicWALL security appliance handles the translation between the private and public address. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive via the WAN interface.

Below, you create the entry as well as the rule to allow HTTP access to the server. You need to create the access policy that allows anyone to make HTTP connections to the webserver via the webserver's public IP address.



### Note

With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your server in). Click on the 'Add...' button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

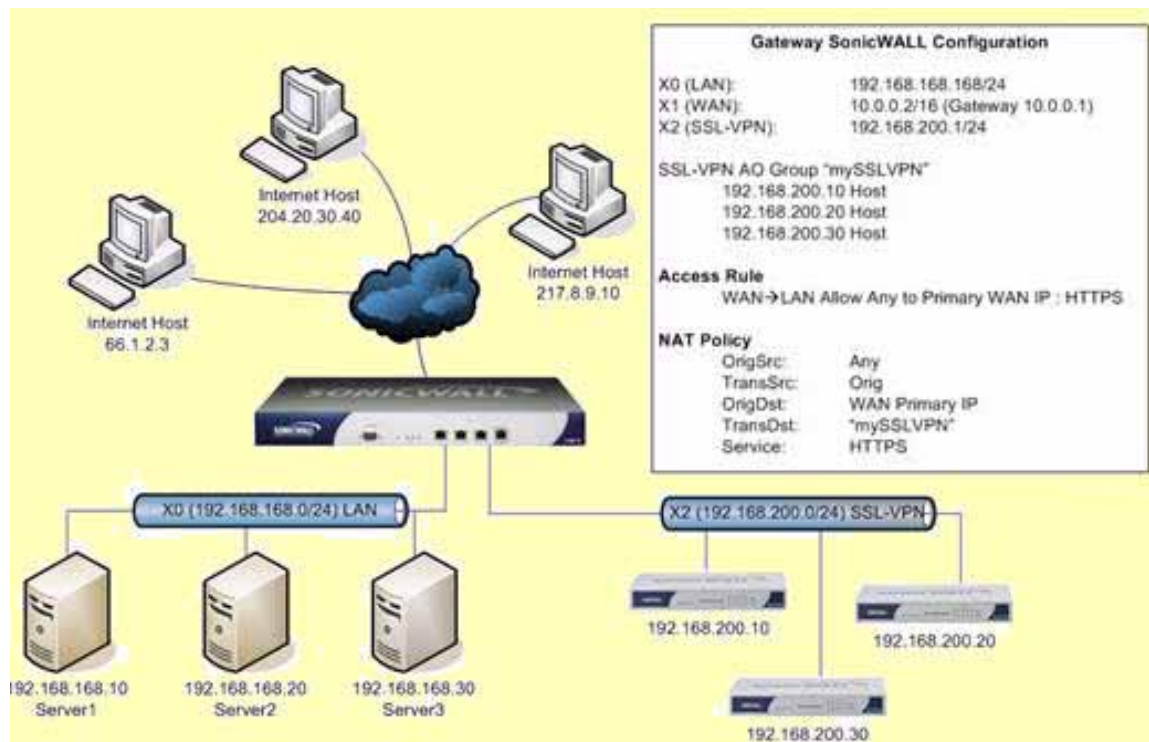
- **Action:** Allow
- **Service:** HTTP
- **Source:** Any
- **Destination:** Webserver\_public\_ip
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** Checked
- **Comment:** (Enter a short description)

When you are done, attempt to access the webserver's public IP address using a system located on the public Internet. You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

## Configuring One-to-Many NAT Load Balancing

One-to-Many NAT policies can be used to persistently load balance the translated destination using the original source IP address as the key to persistence. For example, SonicWALL security appliances can load balance multiple SonicWALL SSL-VPN appliances, while still maintaining session persistence by always balancing clients to the correct destination SSL-VPN. Figure 18.1 shows a sample topology and configuration.

Figure 21:1 One-to-Many NAT Load Balancing Topology and Configuration



To configure One-to-Many NAT load balancing, first go to the **Firewall > Access Rules** page and choose the policy for **WAN** to **LAN**. Click on the **Add...** button to bring up the pop-up access policy screen. When the pop-up appears, enter in the following values:

- **Action:** Allow
- **Service:** HTTPS
- **Source:** Any
- **Destination:** WAN Primary IP
- **Users Allowed:** All
- **Schedule:** Always on
- **Comment:** Descriptive text, such as SSLVPN LB
- **Logging:** Checked
- **Allow Fragmented Packets:** Unchecked

Next, create the following NAT policy by selecting **Network > NAT Policies** and clicking on the **Add...** button:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** Select **Create new address object...** to bring up the **Add Address Object** screen.
  - **Name:** A descriptive name, such as mySSLVPN
  - **Zone assignment:** LAN
  - **Type:** Host

- **IP Address:** The network IP address for the devices to be load balanced (in the topology shown in Figure 18.1, this is 192.168.200.1)
- **Original Service:** HTTPS
- **Translated Service:** HTTPS
- **Inbound Interface:** Any
- **Outbound Interface:** Any
- **Comment:** Descriptive text, such as SSLVPN LB
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

## Inbound Port Address Translation via One-to-One NAT Policy

This type of NAT policy is useful when you want to conceal an internal server's real listening port, but provide public access to the server on a different port. In the example below, you modify the NAT policy and rule created in the previous section to allow public users to connect to the private webserver on its public IP address, but via a different port (TCP 9000), instead of the standard HTTP port (TCP 80).

- 
- Step 1** Create a custom service for the different port. Go to the **Firewall > Custom Services** page and select the **Add** button. When the pop-up screen appears, give your custom service a name such as **webserver\_public\_port**, enter in **9000** as the starting and ending port, and choose **TCP(6)** as the protocol. When done, click on the **OK** button to save the custom service.
- Step 2** Modify the NAT policy created in the previous section that allowed any public user to connect to the webserver on its public IP address. Go to the **Network > NAT Policies** menu and click on the Edit button next to this NAT policy. The Edit NAT Policy window is displayed for editing the policy. Edit the NAT policy so that it includes the following from the drop-down menus:
- **Original Source:** Any
  - **Translated Source:** Original
  - **Original Destination:** webserver\_public\_ip
  - **Translated Destination:** webserver\_private\_ip
  - **Original Service:** webserver\_public\_port (or whatever you named it above)
  - **Translated Service:** HTTP
  - **Inbound Interface:** WAN
  - **Outbound Interface:** Any
  - **Comment:** Enter a short description
  - **Enable NAT Policy:** Checked
  - **Create a reflective policy:** Unchecked



**Note** Make sure you chose **Any** as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it's actually the correct thing to do (if you try to specify the interface, you get an error).

**Step 3** When finished, click on the **OK** button to add and activate the NAT Policy. With this policy in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface, and translates the requested protocol (TCP 9000) to the server's actual listening port (TCP 80).

Finally, you're going to modify the firewall access rule created in the previous section to allow any public user to connect to the webserver on the new port (TCP 9000) instead of the server's actual listening port (TCP 80).



**Note** With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** section and choose the policy for the **WAN to Sales** zone intersection (or, whatever zone you put your server in). Click on the **Configure** button to bring up the previously created policy. When the pop-up appears, edit in the following values:

- **Action:** Allow
- **Service:** webserver\_public\_port (or whatever you named it above)
- **Source:** Any
- **Destination:** webserver\_public\_ip
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you're done, attempt to access the webserver's public IP address using a system located on the public Internet on the new custom port (example: <http://67.115.118.70:9000>). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

## Inbound Port Address Translation via WAN IP Address

This is one of the more complex NAT policies you can create on a SonicWALL security appliance running SonicOS Enhanced – it allows you to use the WAN IP address of the SonicWALL security appliance to provide access to multiple internal servers. This is most useful in situations where your ISP has only provided a single public IP address, and that IP address has to be used by the SonicWALL security appliance's WAN interface.

Below, you create the programming to provide public access to two internal web servers via the SonicWALL security appliances WAN IP address; each is tied to a unique custom port. In the following examples, you set up two, but it's possible to create more than these as long as the ports are all unique.

In this section, we have five tasks to complete:

1. Create two custom service objects for the unique public ports the servers respond on.
2. Create two address objects for the servers' private IP addresses.

3. Create two NAT entries to allow the two servers to initiate traffic to the public Internet.
4. Create two NAT entries to map the custom ports to the actual listening ports, and to map the private IP addresses to the SonicWALL's WAN IP address.
5. Create two access rule entries to allow any public user to connect to both servers via the SonicWALL's WAN IP address and the servers' respective unique custom ports.

---

**Step 1** Create a custom service for the different port. Go to the **Firewall > Custom Services** page and click on the Add button. When the pop-up screen appears, give your custom services names such as **servone\_public\_port** and **servtwo\_public\_port**, enter in **9100** and **9200** as the starting and ending port, and choose **TCP(6)** as the protocol. When done, click on the **OK** button to save the custom services.

**Step 2** Go to the **Network > Address Objects** and click on the **Add** button at the bottom of the page. In the **Add Address Objects** window, enter in a description for server's private IP addresses, choose **Host** from the drop-down box, enter the server's private IP addresses, and select the zone that the servers are in. When done, click on the **OK** button to create the range object.

**Step 3** Go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create a NAT policy to allow the two servers to initiate traffic to the public Internet using the SonicWALL security appliance's WAN IP address, choose the following from the drop-down boxes:

- **Original Source:** servone\_private\_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** servtwo\_private\_ip
- **Translated Source:** WAN Primary IP
- **Original Destination:** Any
- **Translated Destination:** Original
- **Original Service:** Any
- **Translated Service:** Original
- **Inbound Interface:** Opt
- **Outbound Interface:** WAN
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

When finished, click on the **OK** button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the servers' private IP addresses to the public IP address when it initiates traffic out the WAN interface.

**Step 4** Go to the **Network > NAT Policies** menu and click on the **Add** button. The **Add NAT Policy** window is displayed. To create the NAT policies to map the custom ports to the servers' real listening ports and to map the SonicWALL's WAN IP address to the servers' private addresses, choose the following from the drop-down boxes:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servone\_private\_ip
- **Original Service:** servone\_public\_port
- **Translated Service:** HTTP
- **Inbound Interface:** WAN
- **Outbound Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked

And:

- **Original Source:** Any
- **Translated Source:** Original
- **Original Destination:** WAN Primary IP
- **Translated Destination:** servtwo\_private\_ip
- **Original Service:** servtwo\_public\_port
- **Translated Service:** HTTP
- **Source Interface:** WAN
- **Destination Interface:** Any
- **Comment:** Enter a short description
- **Enable NAT Policy:** Checked
- **Create a reflective policy:** Unchecked



**Note** Make sure you choose 'Any' as the destination interface, and not the interface that the server is on. This may seem counter-intuitive, but it's actually the correct thing to do (if you try to specify the interface, you get an error).

When finished, click on the 'OK' button to add and activate the NAT policies. With these policies in place, the SonicWALL security appliance translates the server's public IP address to the private IP address when connection requests arrive from the WAN interface.

**Step 5** Create the access rules that allows anyone from the public Internet to access the two web servers using the custom ports and the SonicWALL security appliance's WAN IP address.



**Note** With previous versions of firmware, it was necessary to write rules to the private IP address. This has been changed as of SonicOS 2.0 Enhanced. If you write a rule to the private IP address, the rule does not work.

Go to the **Firewall > Access Rules** page and choose the policy for the 'WAN' to 'Sales' zone intersection (or, whatever zone you put your servers in). Click on the 'Add...' button to bring up the pop-up window to create the policies. When the pop-up appears, enter the following values:

- **Action:** Allow
- **Service:** servone\_public\_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP Address
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

And:

- **Action:** Allow
- **Service:** servtwo\_public\_port (or whatever you named it above)
- **Source:** Any
- **Destination:** WAN IP Address
- **Users Allowed:** All
- **Schedule:** Always on
- **Logging:** checked
- **Comment:** (enter a short description)

When you're finished, attempt to access the web servers via the SonicWALL's WAN IP address using a system located on the public Internet on the new custom port (example: `http://67.115.118.70:9100` and `http://67.115.118.70:9200`). You should be able to successfully connect. If not, review this section, and the section before, and ensure that you have entered in all required settings correctly.

## Using NAT Load Balancing

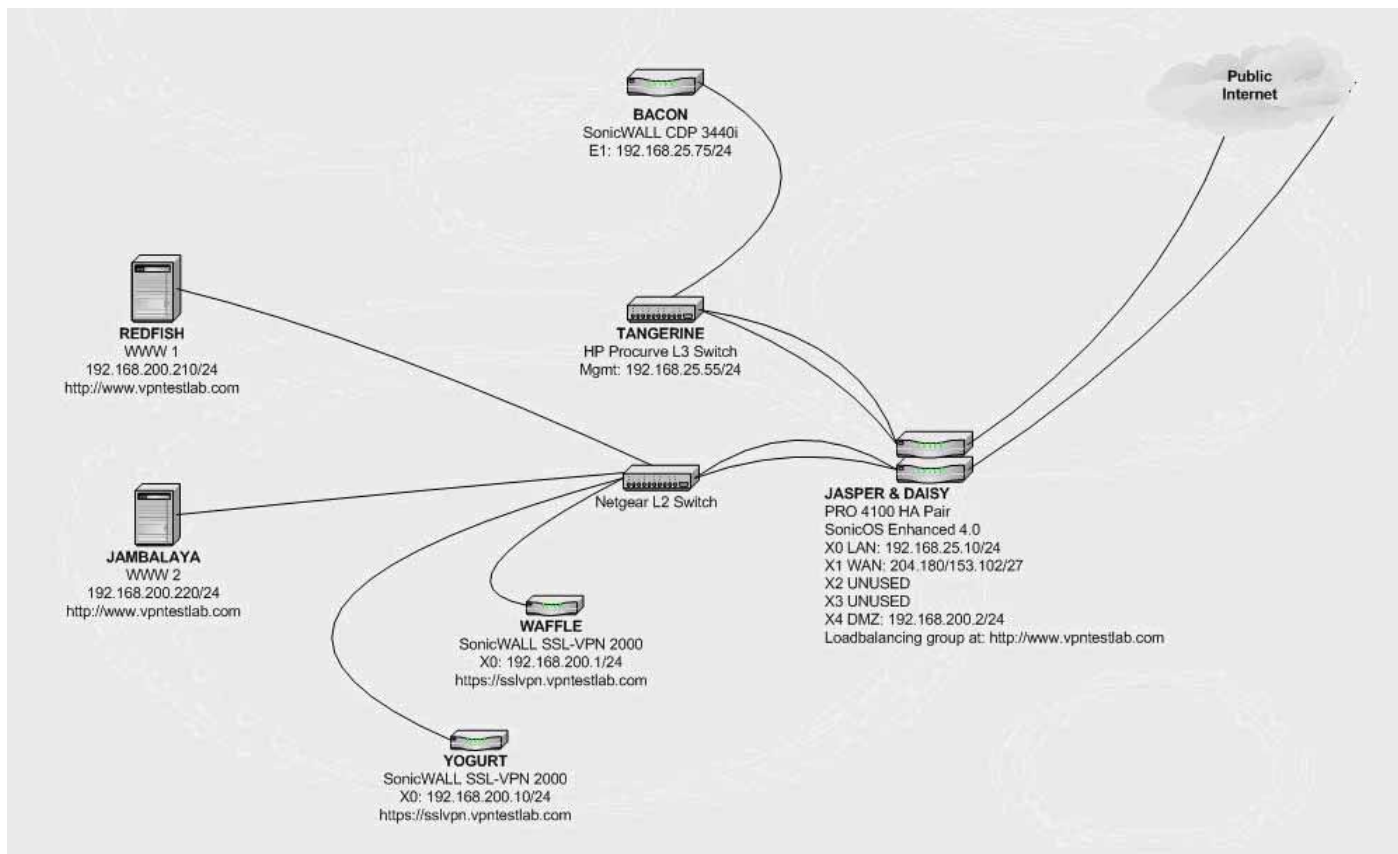
This section contains the following subsections:

- ["NAT Load Balancing Topology" on page 263](#)
- ["Prerequisites" on page 264](#)
- ["Configuring NAT Load Balancing" on page 265](#)
- ["Troubleshooting NAT Load Balancing" on page 269](#)

### NAT Load Balancing Topology

Figure 1 shows the topology for the NAT load balancing network.

Figure 1 NAT Load Balancing Topology



## Prerequisites

The examples shown in the **Tasklist** section on the next few pages utilize IP addressing information from a demo setup – please make sure and replace any IP addressing information shown in the examples with the correct addressing information for your setup. Also note that the interface names may be different.



### Note

It is strongly advised that you enable logging for all categories, and enable name resolution for logging.

To enable logging and alerting, log into the SonicWALL's Management GUI, go to **Log > Categories**, choose **Debug** from the drop-down next to **Logging Level**, chose **All Categories** from the drop-down next to **View Style**, check the boxes in the title bar next to **Log** and **Alerts** to capture all categories, and click on the **Apply** button in the upper right hand corner to save



and activate the changes. For an example, see the screenshot below. Debug logs should only be used for initial configuration and troubleshooting, and it is advised that once setup is complete, you set the logging level to a more appropriate level for your network environment.

**Log Severity/Priority**

Logging Level:  Log Redundancy Filter (seconds):

Alert Level:  Alert Redundancy Filter (seconds):

**Log Categories**

View Style:

Category	Description	Log	Alerts	Syslog	Event Count
----------	-------------	-----	--------	--------	-------------

To enable log name resolution, go to **Log > Name Resolution**, choose **DNS then NetBios** from the **Name Resolution Menu** drop-down list, and click on the **Apply** button in the upper right hand corner to save and activate the changes.

**Name Resolution Settings**

Name Resolution Method:

## Configuring NAT Load Balancing

To configure NAT load balancing, you must complete the following tasks:

1. Create address objects.
2. Create address group.
3. Create inbound NAT LB Policy.
4. Create outbound NAT LB Policy.
5. Create Firewall Rule.
6. Verify and troubleshoot the network if necessary.

To complete this configuration, perform the following steps:

- Step 1 Create Network Objects --** Go to the **Network > Address Objects** page in the Management GUI and create the network objects for both of the internal Web servers, and the Virtual IP (VIP) on which external users will access the servers.

Name:

Zone Assignment:

Type:

IP Address:

Ready

Name:

Zone Assignment:

Type:

IP Address:

Ready

Name:

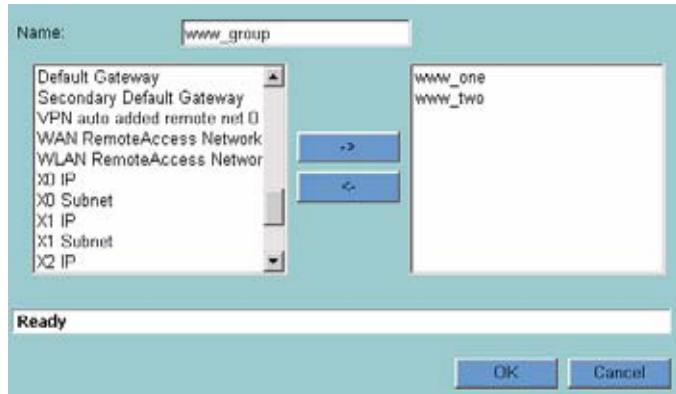
Zone Assignment:

Type:

IP Address:

Ready

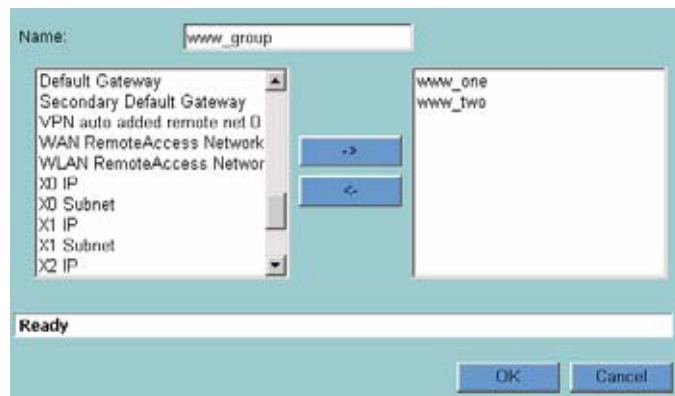
**Step 2 Create Address Group** -- Now create an address group named **www\_group** and add the two internal server address objects you just created.



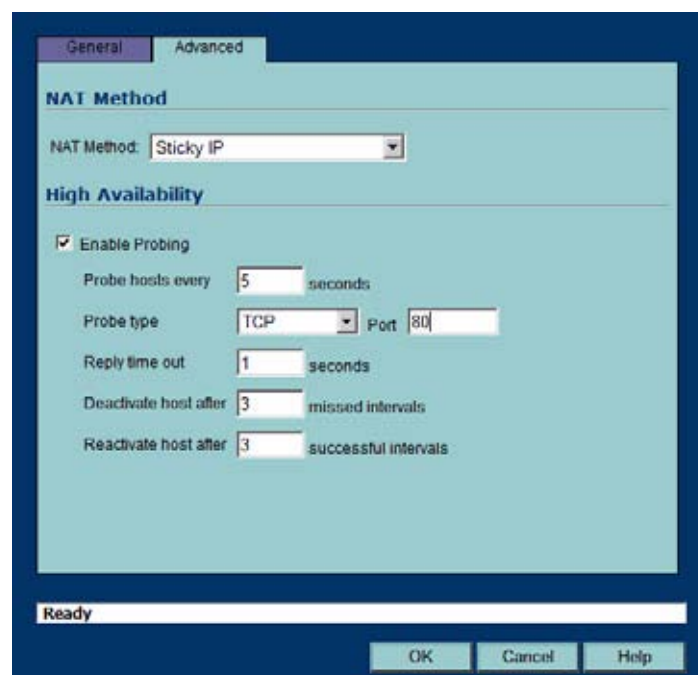
**Step 3 Create Inbound NAT Rule for Group** -- Now create a NAT rule to allow anyone attempting to access the VIP to get translated to the address group you just created, using **Sticky IP** as the NAT method. For an example see the screenshot below.



**Note** Do not save the NAT rule just yet.



**Step 4 Set LB Type and Server Liveliness Method** -- On the **Advanced** tab of the NAT policy configuration control, you can specify that the object (or group of objects, or group of groups) be monitored via ICMP ping or by checking for TCP sockets opened. For this example, we are going to check to see if the server is up and responding by monitoring TCP port 80 (which is good, since that is what people are trying to access). You can now click on the **OK** button to save and activate the changes.





**Note**

Before you go any further, check the logs and the status page to see if the resources have been detected and have been logged as online. If you do not see the two messages below (with your IP addresses), check the steps above.

22	12/13/2006 13:18:49.096	Alert	Firewall Event	Network Monitor: Host 192.168.200.220 is online
23	12/13/2006 13:18:49.096	Alert	Firewall Event	Network Monitor: Host 192.168.200.210 is online

Latest Alerts	
Date/Time	Message
12/13/2006 13:18:49	Network Monitor: Host 192.168.200.220 is online
12/13/2006 13:18:49	Network Monitor: Host 192.168.200.210 is online

**Step 5 Create Outbound NAT Rule for LB Group --** Write a NAT rule to allow the internal servers to get translated to the VIP when accessing resources out the WAN interface.

**NAT Policy Settings**

Original Source:

Translated Source:

Original Destination:

Translated Destination:

Original Service:

Translated Service:

Inbound Interface:

Outbound Interface:

Comment:

Enable NAT Policy

Create a reflexive policy

Ready

OK Cancel Help

- Step 6 Create Firewall Rule for VIP** -- Write a firewall rule to allow traffic from the outside to access the internal Web servers via the VIP.

General | **Advanced** | QoS

**Settings**

Action:  Allow  Deny  Discard

From Zone: WAN

To Zone: DMZ

Service: HTTP

Source: Any

Destination: www\_public

Users Allowed: All

Schedule: Always on

Comment: allow access to www lb group

Enable Logging

Allow Fragmented Packets

Ready

OK Cancel Help

- Step 7 Test Your Work** – From a laptop outside the WAN, connect via HTTP to the VIP using a Web browser.



**Note**

If you wish to load balance one or more SSL-VPN Appliances, repeat steps 1-7, using HTTPS instead as the allowed service.

## Troubleshooting NAT Load Balancing

If the Web servers do not seem to be accessible, go to the **Firewall > Access Rules** page and mouse-over the **Statistics** icon.

If the rule is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

Access Rules (WAN > DMZ) Items: 1 to 2 (of 2)

View Style:  All Rules  Matrix  Drop-down Boxes

#	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	1	Any	www_public	HTTP	Allow	All		<input checked="" type="checkbox"/>	
2	2	Any	Any	Any	Deny	All		<input type="checkbox"/>	

Access Rule #1 - Traffic Statistics

- Rx Bytes: 10335
- Rx Packets: 20
- Tx Bytes: 5821
- Tx Packets: 27

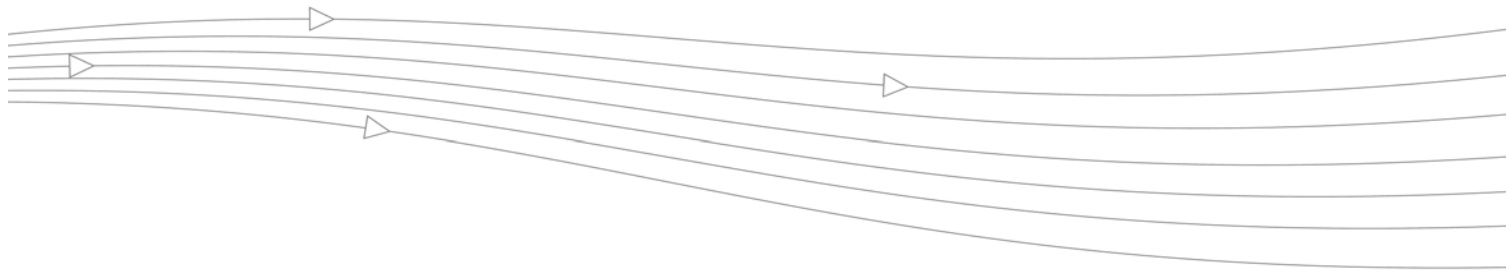
Add... Delete Restore Defaults...

You can also check the **Firewall > NAT Policies** page and mouse-over the **Statistics** icon. If the policy is configured incorrectly you will not see any Rx or TX Bytes; if it is working, you will see these increment with each successful external access of the load balanced resources.

The screenshot displays the NAT Policies configuration interface. At the top, it shows 'Items: 1 to 6 (of 6)'. Below the title, there are radio buttons for 'View Style: All Policies', 'Custom Policies', and 'Default Policies'. The main area contains a table with the following columns: #, Source (Original, Translated), Destination (Original, Translated), Service (Original, Translated), Interface (Inbound, Outbound), Priority, Comment, Enable, and Configure. There are 6 rows of policies. A tooltip for policy #1 is open, showing statistics: Usage Count: 2, Rx Bytes: 10336, Rx Packets: 20, Tx Bytes: 5021, Tx Packets: 27. At the bottom, there are 'Add...', 'Delete', and 'Delete All' buttons.

#	Source	Destination	Service	Interface	Priority	Comment	Enable	Configure				
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound				
1	Any	Original	www_public	www_group	HTTP	Original	X1	Any	20		<input checked="" type="checkbox"/>	
2	www_group	www_public	Any	Original	Any	Original	X4	Any			<input type="checkbox"/>	
3	Any	X2 IP	Any	Original	Any	Original	X4	X2			<input type="checkbox"/>	
4	Any	X1 IP	Any	Original	Any	Original	X4	X1			<input type="checkbox"/>	
5	Any	X2 IP	Any	Original	Any	Original	X0	X2	24		<input checked="" type="checkbox"/>	
6	Any	X1 IP	Any	Original	Any	Original	X0	X1	25		<input checked="" type="checkbox"/>	

Finally, check the logs and the status page to see if there are any alerts (noted in yellow) about the Network Monitor noting hosts that are offline; it may be that all of your load balancing resources are not reachable by the SonicWALL appliance and that the probing mechanism has marked them offline and out of service. Check the load balancing resources to ensure that they are functional and check the networking connections between them and the SonicWALL appliance.



# CHAPTER 22

## Managing ARP Traffic

### Network > ARP

Network > ARP Flush ARP Cache... Apply Cancel ?

Static ARP Entries

#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
<input type="checkbox"/>	1	192.168.50.1	00:06:b1:04:00:e5	X2	<input checked="" type="checkbox"/>	

Add Delete Delete All

ARP Settings

ARP Cache entry timeout (minutes):

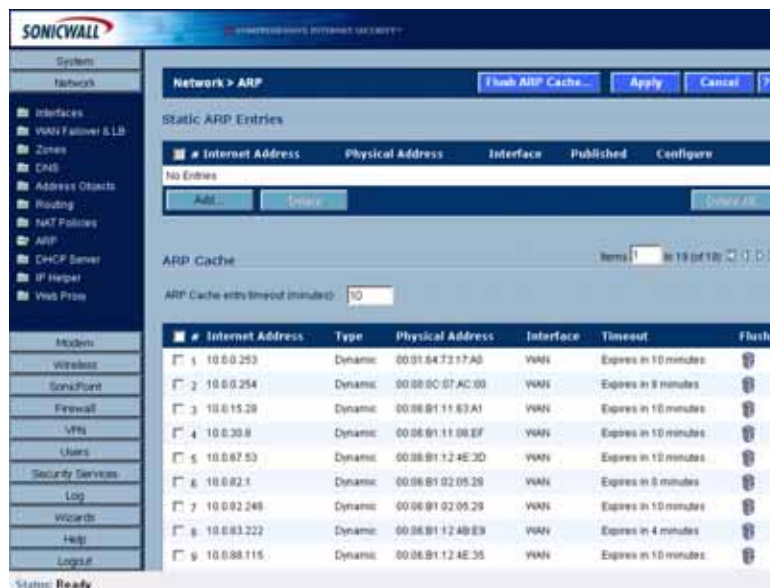
ARP Cache Items 1 to 7 (of 7)

#	IP Address	Type	MAC Address	Interface	Timeout	Flush
<input type="checkbox"/>	1	10.0.93.56	Static	00:06:b1:12:47:D7	X1	Permanent published
<input type="checkbox"/>	2	10.0.202.118	Dynamic	00:00:56:84:99:C9	X1	Expires in 10 minutes
<input type="checkbox"/>	3	172.31.20.1	Static	00:06:b1:12:47:D9	X3 V20	Permanent published
<input type="checkbox"/>	4	175.31.16.1	Static	00:06:b1:12:47:DA	X4	Permanent published
<input type="checkbox"/>	5	192.168.50.1	Static	00:06:b1:04:00:E5	X2	Permanent published
<input type="checkbox"/>	6	192.168.100.1	Static	00:06:b1:12:47:D9	X3 V100	Permanent published
<input type="checkbox"/>	7	192.168.168.168	Static	00:06:b1:12:47:D6	X0	Permanent published

Flush Flush ARP Cache

ARP Statistics: ARP Statistics: 7 entries, 1381 lookups, 6 failures, 1363 hits, 12 misses, 99% hit rate

ARP (Address Resolution Protocol) maps layer 3 (IP addresses) to layer 2 (physical or MAC addresses) to enable communications between hosts residing on the same subnet. ARP is a broadcast protocol that can create excessive amounts of network traffic on your network. To minimize the broadcast traffic, an ARP cache is maintained to store and reuse previously learned ARP information.



## Static ARP Entries

The Static ARP feature allows for static mappings to be created between layer 2 MAC addresses and layer 3 IP addresses, but also provides the following capabilities:



- **Publish Entry** - Enabling the **Publish Entry** option in the **Add Static ARP** window causes the SonicWALL device to respond to ARP queries for the specified IP address with the specified MAC address. This can be used, for example, to have the SonicWALL device reply for a secondary IP address on a particular interface by adding the MAC address of the SonicWALL. See the Secondary Subnet section that follows.
- **Bind MAC Address** - Enabling the **Bind MAC Address** option in the **Add Static ARP** window binds the MAC address specified to the designated IP address and interface. This can be used to ensure that a particular workstation (as recognized by the network card's unique MAC address) can only be used on a specified interface on the SonicWALL. Once the MAC address is bound to an interface, the SonicWALL will not respond to that MAC



address on any other interface. It will also remove any dynamically cached references to that MAC address that might have been present, and it will prohibit additional (non-unique) static mappings of that MAC address.

- **Update IP Address Dynamically** - The **Update IP Address Dynamically** setting in the Add Static ARP window is a sub-feature of the **Bind MAC Address** option. This allows for a MAC address to be bound to an interface when DHCP is being used to dynamically allocate IP addressing. Enabling this option will blur the IP Address field, and will populate the ARP Cache with the IP Address allocated by the SonicWALL's internal DHCP server, or by the external DHCP server if IP Helper is in use.

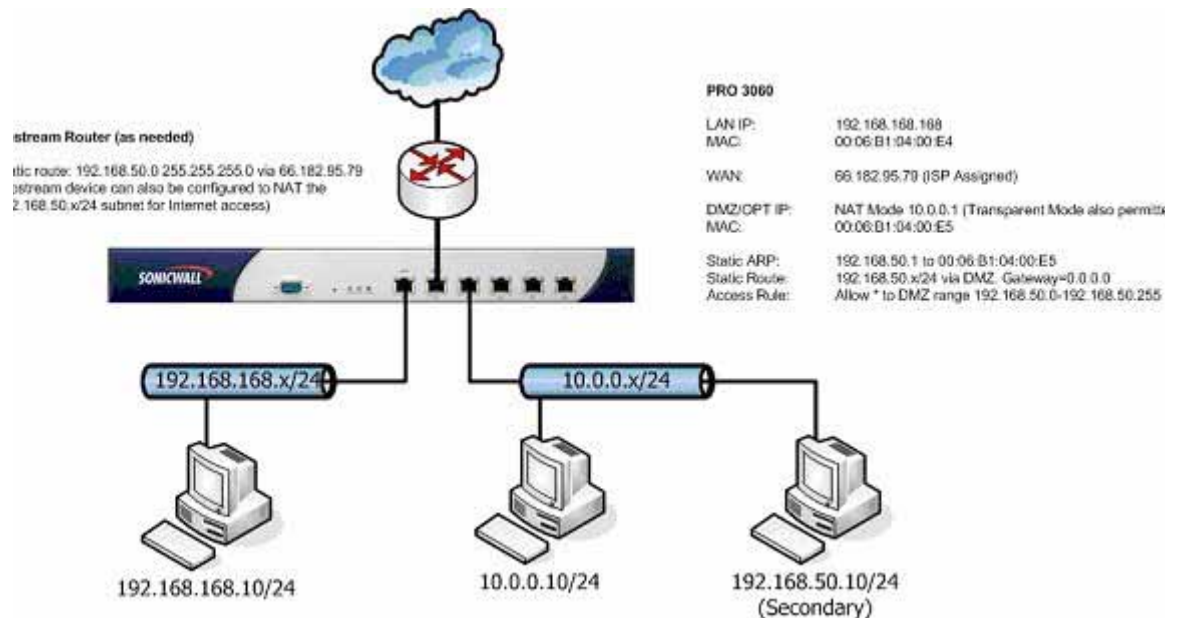
## Secondary Subnets with Static ARP

The Static ARP feature allows for secondary subnets to be added on other interfaces, and without the addition of automatic NAT rules.

### Adding a Secondary Subnet using the Static ARP Method

- Step 1** Add a 'published' static ARP entry for the gateway address that will be used for the secondary subnet, assigning it the MAC address of the SonicWALL interface to which it will be connected.
- Step 2** Add a static route for that subnet, so that the SonicWALL regards it as valid traffic, and knows to which interface to route that subnet's traffic.
- Step 3** Add Access Rules to allow traffic destined for that subnet to traverse the correct network interface.
- Step 4** Optional: Add a static route on upstream device(s) so that they know which gateway IP to use to reach the secondary subnet.

Consider the following network example:



To support the above configuration, first create a published static ARP entry for 192.168.50.1, the address which will serve as the gateway for the secondary subnet, and associate it with the DMZ/OPT interface. From the **Network > ARP** page, select the **Add** button in the **Static ARP Entries** section, and add the following entry:

The entry will appear in the table as follows:

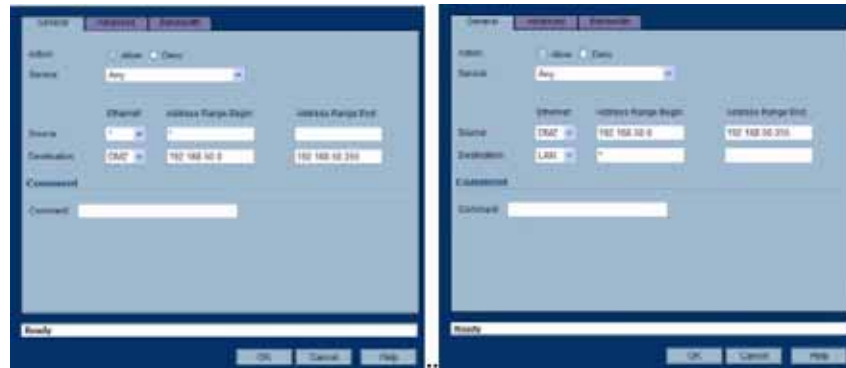
#	IP Address	MAC Address	Interface	Published	Bind MAC	Configure
1	192.168.50.1	00:06:b1:04:00:e5	X2	✓		

Navigate to the **Network > Routing** page, and add a static route for the 192.168.50.0/24 network as follows:

The entry will appear in the table as follows:

Destination Network	Subnet Mask	Gateway	Interface	Configure
192.168.50.0	255.255.255.0	0.0.0.0	OPT	

To allow the traffic to reach the 192.168.50.0/24 subnet, and to allow the 192.168.50.0/24 subnet to reach the hosts on the LAN, navigate to the **Firewall > Access Rules** page, and add the following Access Rule:



## Navigating and Sorting the ARP Cache Table

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table.

#	IP Address	Type	MAC Address	Interface	Timeout	Flush
1	10.0.0.254	Dynamic	00:00:0C:07:AC:00	WAN	expires in 6 mins	🗑️
2	10.0.88.123	Dynamic	00:06:B1:11:05:FA	WAN	expires in 10 mins	🗑️
3	10.0.92.2	Dynamic	00:06:B1:12:44:B3	WAN	expires in 10 mins	🗑️
4	10.0.93.24	Dynamic	00:06:B1:12:51:4D	WAN	expires in 10 mins	🗑️
5	10.0.93.52	Static	00:06:B1:13:5A:C0	WAN	permanent published	🗑️
6	10.0.93.52	Static	00:06:B1:13:5A:C0	OPT	permanent published	🗑️
7	10.0.202.62	Dynamic	00:80:D0:5A:5D:69	WAN	expires in 10 mins	🗑️
8	192.168.168.168	Static	00:06:B1:13:5A:BE	LAN	permanent published	🗑️

ARP Statistics: ARP Statistics: 8 entries, 1129 lookups, 737 failures, 320 hits, 2 misses, 99% hit rate

The navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

## Navigating and Sorting the ARP Cache Table Entries

The **ARP Cache** table provides easy pagination for viewing a large number of ARP entries. You can navigate a large number of ARP entries listed in the **ARP Cache** table by using the navigation control bar located at the top right of the **ARP Cache** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

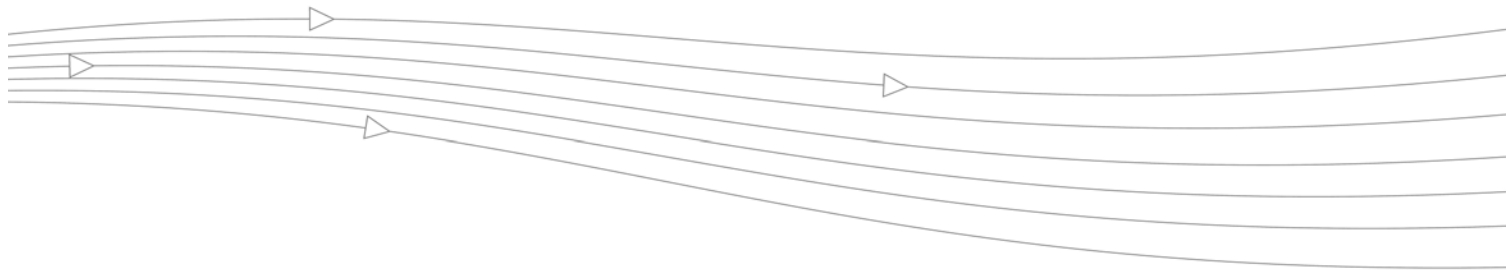
You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific ARP entry. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

## Flushing the ARP Cache

It is sometimes necessary to flush the ARP cache if the IP address has changed for a device on the network. Since the IP address is linked to a physical address, the IP address can change but still be associated with the physical address in the ARP Cache. Flushing the ARP Cache allows new information to be gathered and stored in the ARP Cache. Click **Flush ARP** Cache to clear the information.

To configure a specific length of time for the entry to time out, enter a value in minutes in the **ARP Cache entry time out (minutes)** field.



# CHAPTER 23

## Setting Up the DHCP Server

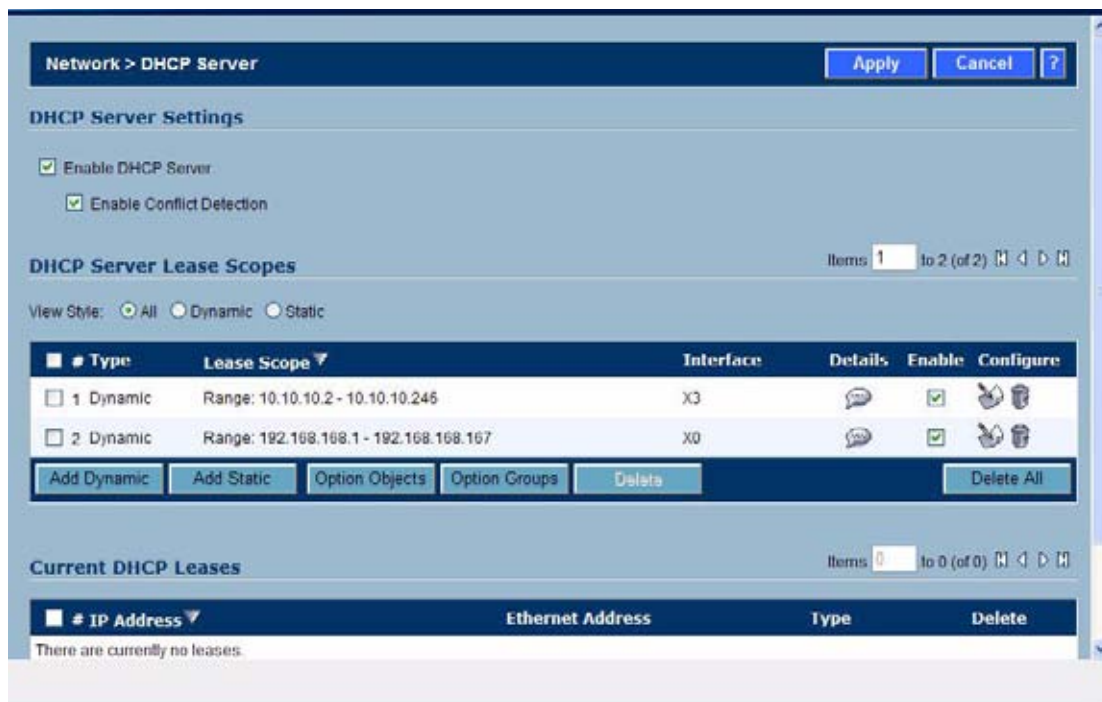
---

### Network > DHCP Server

This chapter contains the following sections:

- [“DHCP Server Options Overview” on page 278](#)
- [“DHCP Server Persistence Overview” on page 279](#)
- [“Enabling the DHCP Server” on page 280](#)
- [“DHCP Server Lease Scopes” on page 280](#)
- [“Configuring DHCP Server for Dynamic Ranges” on page 281](#)
- [“Configuring Static DHCP Entries” on page 283](#)
- [“Configuring SonicWALL DHCP Server Options” on page 285](#)
- [“Current DHCP Leases” on page 294](#)
- [“DHCP Option Numbers” on page 294](#)

The SonicWALL security appliance includes a DHCP (Dynamic Host Configuration Protocol) server to distribute IP addresses, subnet masks, gateway addresses, and DNS server addresses to your network clients. The **Network > DHCP Server** page includes settings for configuring the SonicWALL security appliance's DHCP server.



You can use the SonicWALL security appliance's DHCP server or use existing DHCP servers on your network. If your network uses its own DHCP servers, make sure the **Enable DHCP Server** checkbox is unchecked.

The number of address ranges and IP addresses the SonicWALL DHCP server can assign depends on the model, operating system, and licenses of the SonicWALL security appliance. For example, on a SonicWALL TZ 170 SP Wireless running SonicOS Enhanced, the SonicWALL DHCP Server can assign a total of 64 address ranges with 64 IP addresses each or a total of 4,096 IP addresses.

## DHCP Server Options Overview

This section provides an introduction to DHCP server options feature. This section contains the following subsections:

- [“What Is the SonicWALL DHCP Server Options Feature?” on page 278](#)
- [“Benefits” on page 279](#)
- [“How Does the SonicWALL DHCP Server Options Feature Work?” on page 279](#)
- [“Supported Standards” on page 279](#)

## What Is the SonicWALL DHCP Server Options Feature?

The SonicWALL DHCP server options feature provides support for DHCP options, also known as vendor extensions, as defined primarily in RFCs 2131 and 2132. DHCP options allow users to specify additional DHCP parameters in the form of pre-defined, vendor-specific information that is stored in the options field of a DHCP message. When the DHCP message is sent to

clients on the network, it provides vendor-specific configuration and service information. The [“DHCP Option Numbers” on page 294](#) provides a list of DHCP options by RFC-assigned option number.

## Benefits

The SonicWALL DHCP server options feature provides a simple interface for selecting DHCP options by number or name, making the DHCP configuration process quick, easy, and compliant with RFC-defined DHCP standards.

## How Does the SonicWALL DHCP Server Options Feature Work?

The SonicWALL DHCP server options feature allows definition of DHCP options using a drop-down menu based on RFC-defined option numbers, allowing administrators to easily create DHCP objects and object groups, and configure DHCP generic options for dynamic and static DHCP lease scopes. Once defined, the DHCP option is included in the options field of the DHCP message, which is then passed to DHCP clients on the network, describing the network configuration and service(s) available.

## Supported Standards

The SonicWALL DHCP server options feature supports the following standards:

- RFC 2131 - Dynamic Host Configuration Protocol
- RFC 2132 - DHCP Options and BOOTP Vendor Extensions

## DHCP Server Persistence Overview

- [“What is DHCP Server Persistence?” on page 279](#)
- [“Benefits” on page 279](#)
- [“How Does DHCP Server Persistence Work?” on page 280](#)

## What is DHCP Server Persistence?

DHCP server persistence is the ability of the firewall save DHCP lease information and to provide the client with a predictable IP address that does not conflict with another use on the network, even after a client reboot.

## Benefits

DHCP server persistence provides a seamless experience when a user reboots a workstation. The DHCP lease information is saved, and the user retains the same workstation IP address. When a firewall is restarted, usually due to maintenance or an upgrade, DHCP server persistence provides the following benefits:

- IP address uniqueness: Lease information is stored in flash memory, so the risk of assigning the same IP address to multiple users is nullified.
- Ease of use: By saving the lease information in the flash memory, the user’s connections are automatically restored.

## How Does DHCP Server Persistence Work?

DHCP server persistence works by storing DHCP lease information periodically to flash memory. This ensures that users have predictable IP addresses and minimizes the risk of IP addressing conflicts after a reboot.


## Enabling the DHCP Server

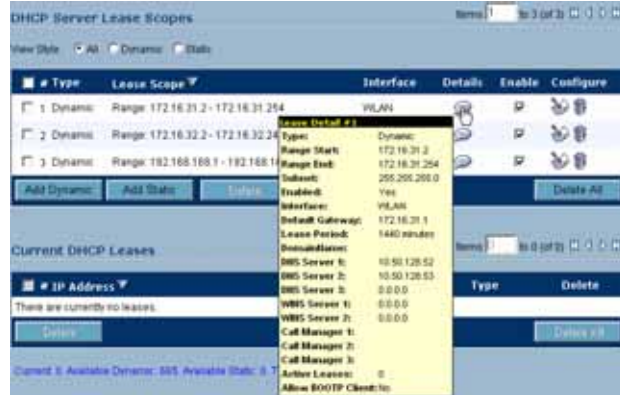
If you want to use the SonicWALL security appliance's DHCP server, select **Enable DHCP Server** on the **Network > DHCP Server** page.


Select **Enable Conflict Detection** to turn on automatic DHCP scope conflict detection on each zone.

## DHCP Server Lease Scopes

The DHCP **Server Lease Scopes** table displays the currently configured DHCP IP ranges. The table shows:

- **Type:** Dynamic or Static
- **Lease Scope:** The IP address range, for example **172.16.31.2 - 172.16.31.254**
- **Interface:** The Interface the range is assigned to--**LAN**, **OPT**, or **WLAN**
- **Details:** Detailed information about the lease, displayed as a tool tip when you hover the mouse pointer over the Details icon 



- **Enable:** Check the box in the Enable column to enable the DHCP range. Uncheck it to disable the range
- **Configure:** Click the configure icon  to configure the DHCP range



## Configuring DHCP Server for Dynamic Ranges

To configure DHCP server for dynamic IP address ranges, follow these instructions:

- Step 1** In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Dynamic**. The **Dynamic Ranges Configuration** window is displayed.



### General Settings

- Step 2** In the **General** page, make sure the **Enable this DHCP Range** is checked, if you want to enable this range.
- Step 3** Select the interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.



**Note** To select an interface from the Interface menu, it must first be fully configured and it must be of the Zone type, LAN, WLAN, or DMZ.

- Step 4** Use the default IP address range entries for the interface in the **Range Start** and **Range End** fields or type in your own IP address range.
- Step 5** Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- Step 6** Select the gateway from the **Gateway Preferences** menu. The interface IP address is the default value, but you can select **Other** and type a different IP address for the gateway.
- Step 7** If you select the interface IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the **Default Gateway** and **Subnet Mask** information into the fields.
- Step 8** Select **Allow BOOTP Clients to use Range** if you have BOOTP Clients on your network.

BOOTP stands for bootstrap protocol, which is a TCP/IP protocol and service that allows diskless workstations to obtain their IP address, other TCP/IP configuration information, and their boot image file from a BOOTP server.

## DNS/WINS Settings

**Step 9** Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



**Step 10** If you have a domain name for the DNS server, type it in the **Domain Name** field.

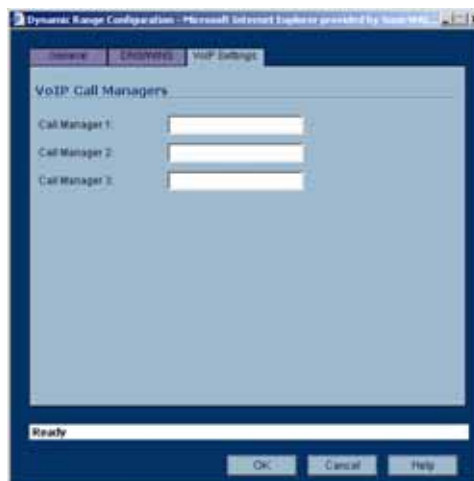
**Step 11** **Inherit DNS Settings Dynamically using SonicWALL's DNS Settings** automatically populates the DNS and WINS settings with the settings in the **Network > DNS** page. This option is selected by default.

**Step 12** If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.

**Step 13** If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can add an additional WINS server.

## VoIP Settings

- Step 14** Click on the **VoIP Settings** tab. The **VoIP Settings** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.



- Step 15** Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

- Step 16** Click **OK** to add the settings to the SonicWALL security appliance.

- Step 17** Click **Apply** for the settings to take effect on the SonicWALL security appliance.

For more information on VoIP support features on the SonicWALL security appliance, see Chapter 28 Configuring VoIP Support.

## Configuring Static DHCP Entries

Static entries are IP addresses assigned to servers requiring permanent IP settings. To configure static entries, follow these steps:

- Step 1** In the **Network > DHCP Server** page, at the bottom of the **DHCP Server Lease Scopes** table, click **Add Static**. The **Static Entry Configuration** window is displayed.



## General Settings

- Step 2** In the **General** tab, make sure the **Enable this DHCP Entry** is checked, if you want to enable this range.
- Step 3** Select the interface from the Interface menu. The IP addresses are in the same private subnet as the selected interface.
- Step 4** Enter a name for the static DNS entry in the **Entry Name** field.
- Step 5** Type the device IP address in the **Static IP Address** field.
- Step 6** Type the device Ethernet (MAC) address in the **Ethernet Address** field.
- Step 7** Type the number of minutes an IP address is used before it is issued another IP address in the **Lease Time (minutes)** field. **1440** minutes (24 hours) is the default value.
- Step 8** Select the gateway from the **Gateway Preferences** menu. The interface IP address is the default value, but you can select **Other** and type a different IP address for the gateway.
- Step 9** If you select the SonicWALL security appliance LAN IP address from the **Gateway Preferences** menu, the **Default Gateway** and **Subnet Mask** fields are unavailable. If you select **Other**, the fields are available for you to type the **Default Gateway** and information into the fields.

## DNS/WINS Settings

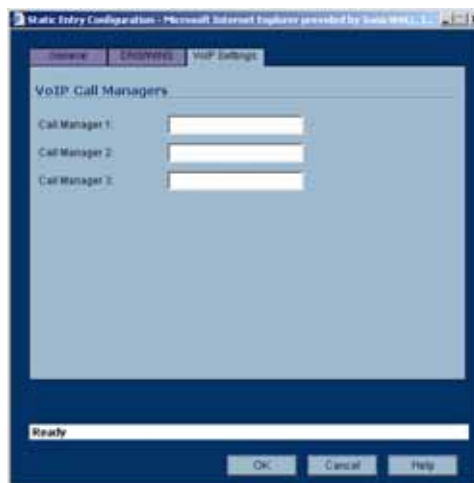
- Step 10** Click the **DNS/WINS** tab to continue configuring the DHCP Server feature.



- Step 11** If you have a domain name for the DNS Server, type it in the **Domain Name** field.
- Step 12** **Inherit DNS Settings Dynamically from the SonicWALL's DNS settings** is selected by default. When selected, the DNS Server IP fields are unavailable.
- Step 13** If you do not want to use the SonicWALL security appliance network settings, select **Specify Manually**, and type the IP address of your DNS Server in the **DNS Server 1** field. You can specify two additional DNS servers.
- Step 14** If you have WINS running on your network, type the WINS server IP address(es) in the **WINS Server 1** field. You can specify an additional WINS server.

## VoIP Settings

**Step 15** Click on the **VoIP Settings** tab. The **VoIP Settings** tab allows you to configure the SonicWALL DHCP server to send Cisco Call Manager information to VoIP clients on the network.



**Step 16** Enter the IP address or FQDN of your VoIP Call Manager in the **Call Manager 1** field. You can add two additional VoIP Call Manager addresses.

**Step 17** Click **OK** to add the settings to the SonicWALL.

**Step 18** Click **Apply** for the settings to take effect on the SonicWALL.

For more information on VoIP support features on the SonicWALL security appliance, see Chapter 28 Configuring VoIP Support.

## Configuring SonicWALL DHCP Server Options

This section provides configuration tasks for DHCP option objects, DHCP option groups, and DHCP generic options for lease scopes. This section contains the following subsections:

- [“Configuring DHCP Option Objects” on page 286](#)
- [“Configuring DHCP Option Groups” on page 290](#)
- [“Configuring DHCP Generic Options for DHCP Lease Scopes” on page 292](#)

The [“DHCP Option Numbers” on page 294](#) provides a list of DHCP options by RFC-assigned option number.

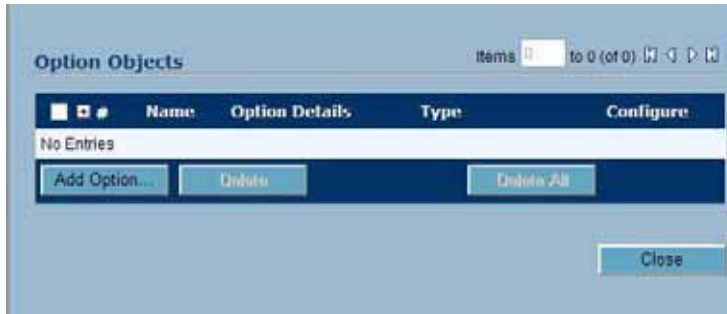
## Configuring DHCP Option Objects

To configure DHCP option objects, perform the following steps:

- Step 1** In the left-hand navigation panel, navigate to **Network > DHCP Server**.



- Step 2** Under DHCP Server Lease Scopes, click the **Option Objects** button. The Option Objects page displays.



- Step 3** Click the **Add Option** button. The Add DHCP Option Objects page displays.

Option Name:

Option Number: 2 (Time Offset) ▼

Option Array

Option Type: Four Byte Data ▼

Option Value:

Ready

OK Cancel

**Step 4** Type a name for the option in the **Option Name** field.

Option Name: DNS server

Option Number: 2 (Time Offset) ▼

Option Array

Option Type: Four Byte Data ▼

Option Value:

Ready

OK Cancel

**Step 5** From the **Option Number** drop-down list, select the option number that corresponds to your DHCP option. For a list of option numbers and names, refer to [“DHCP Option Numbers” on page 294](#).

Option Name: DNS server

Option Number: 5 (DNS Servers) ▼

Option Array

Option Type: IP Address ▼

Option Value:

Ready

OK Cancel

- Step 6** Optionally check the **Option Array** box to allow entry of multiple option values in the **Option Value** field.

The image shows a configuration dialog box for a DHCP server option. The fields are as follows:

- Option Name: DNS server
- Option Number: 6 (DNS Servers)
- Option Array:
- Option Type: IP Address
- Option Value: (Empty text area)
- Status: Ready
- Buttons: OK, Cancel



- Step 7** The option type displays in the **Option Type** drop-down menu. If only one option type is available, for example, for Option Number **2 (Time Offset)**, the drop-down menu will be greyed out. If there are multiple option types available, for example, for Option Number **77 (User Class Information)**, the drop-down menu will be functional.

Option Number: 2 (Time Offset) [v]  
 Option Array  
 Option Type: Four Byte Data [v]

Option Number: 77 (User Class Information) [v]  
 Option Array  
 Option Type: Four Byte Data [v]

- Step 8** Type the option value, for example, an IP address, in the **Option Value** field. If **Option Array** is checked, multiple values may be entered, separated by a semi-colon (;).

Option Name: DNS server  
 Option Number: 6 (DNS Servers) [v]  
 Option Array  
 Option Type: IP Address [v]  
 Option Value: 10.0.1.1;10.0.1.2;10.0.1.3  
 Ready  
 OK Cancel

- Step 9** Click **OK**. The object will display in the Option Objects list.

Option Objects Items 1 to 1 (of 1) [v] [v] [v] [v]

#	Name	Option Details	Type	Configure
1	DNS server	6/10.0.1.1;10.0.1.2;10.0.1.3	IP Address	[v] [v]

Add Option... Delete Delete All Close

## Configuring DHCP Option Groups

To configure DHCP option groups, perform the following steps:

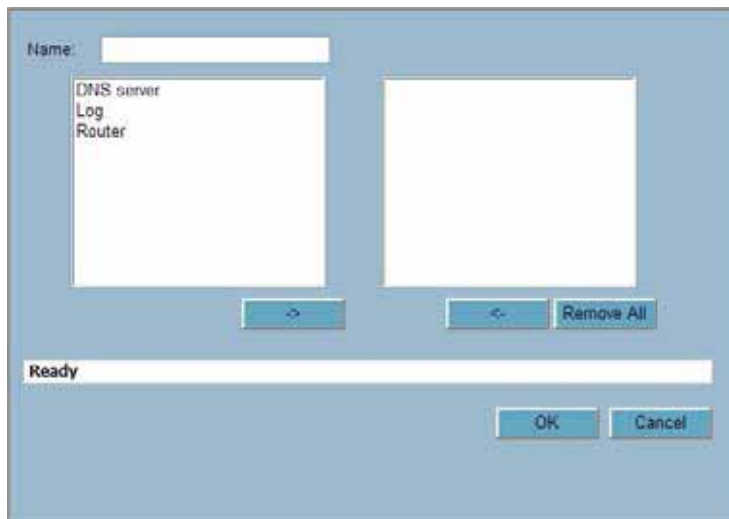
**Step 1** In the left-hand navigation panel, navigate to **Network > DHCP Server**.



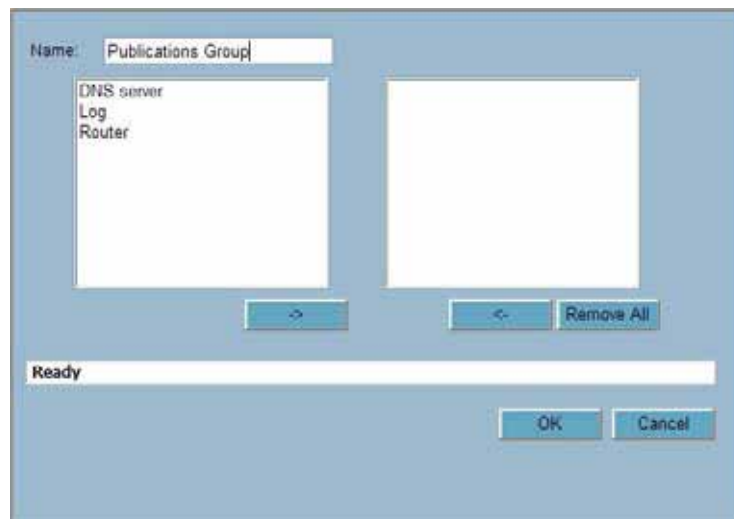
**Step 2** Under DHCP Server Lease Scopes, click **Option Groups**. The Option Groups page displays.



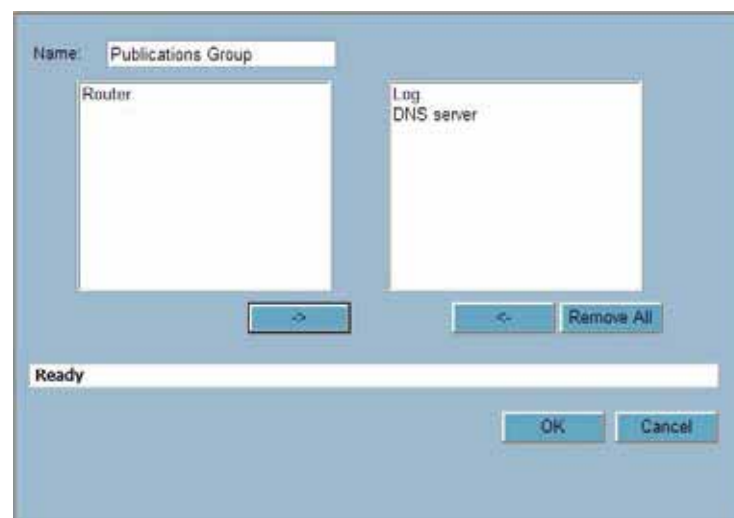
**Step 3** Click the **Add Group** button. The Add DHCP Option Group page displays.



**Step 4** Enter a name for the group in the **Name** field.



**Step 5** Select an option object from the left column and click the -> button to add it to the group. To select multiple option objects at the same time, hold the **Ctrl** key while selecting the option objects.



**Step 6** Click **OK**. The group displays in the Option Groups list.



## Configuring DHCP Generic Options for DHCP Lease Scopes

**Note**

Before generic options for a DHCP lease scope can be configured, a static or dynamic DHCP server lease scope must be created.

To configure DHCP generic options for DHCP server lease scopes, perform the following tasks:

- Step 1** If modifying an existing DHCP lease scope, locate the lease scope under DHCP Server Lease Scopes on the **Network > DHCP Server** page and click the configure icon, then click the **Advanced** tab. If creating a new DHCP lease scope, click the **Advanced** tab.

The screenshot shows the configuration window for a DHCP lease scope, with the 'Advanced' tab selected. The window has three tabs: 'General', 'DNS/WINS', and 'Advanced'. The 'Advanced' tab is active and displays the following configuration options:

- VoIP Call Managers:** Three input fields for 'Call Manager 1:', 'Call Manager 2:', and 'Call Manager 3:'.
- DHCP Generic Options:**
  - A dropdown menu for 'DHCP Generic Option Group' is set to 'None'.
  - A checkbox labeled 'Send Generic options always' is currently unchecked.

At the bottom of the window, there is a status bar showing 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'.

**Step 2** Select a DHCP option or option group in the **DHCP Generic Option Group** drop-down menu.

The screenshot shows a configuration dialog box with three tabs: General, DNS/WINS, and Advanced. The Advanced tab is selected. Under the heading "VoIP Call Managers", there are three text input fields labeled "Call Manager 1:", "Call Manager 2:", and "Call Manager 3:". Below this, under the heading "DHCP Generic Options", there is a dropdown menu labeled "DHCP Generic Option Group:" with "Publications Group" selected. A checkbox labeled "Send Generic options always" is currently unchecked. At the bottom of the dialog, there is a status bar showing "Ready" and three buttons: "OK", "Cancel", and "Help".

**Step 3** To always use DHCP options for this DHCP server lease scope, check the box next to **Send Generic options always**.

This screenshot is identical to the previous one, but the checkbox labeled "Send Generic options always" is now checked, indicating that the user has selected this option.

**Step 4** Click **OK**.

## Current DHCP Leases

The current DHCP lease information is displayed in the **Current DHCP Leases** table. Each binding entry displays the **IP Address**, the **Ethernet Address**, and the **Type** of binding (Dynamic, Dynamic BOOTP, or Static BOOTP).

#	IP Address	Ethernet Address	Type	Delete
1	172.16.31.2	00:02:EF:20:BE:29	Dynamic	
2	172.16.32.2	00:90:4B:76:20:3B	Dynamic	
3	172.16.32.3	00:02:EF:20:BE:29	Dynamic	

To delete a binding, which frees the IP address on the DHCP server, click the Delete icon next to the entry. For example, use the Delete icon to remove a host when it has been removed from the network, and you need to reuse its IP address.

## DHCP Option Numbers

This section provides a list of RFC-defined DHCP option numbers and descriptions:

Option Number	Name	Description
2	Time Offset	Time offset in seconds from UTC
3	Router	N/4 router addresses
4	Time Servers	N/4 time server addresses
5	Name Servers	N/4 IEN-116 server addresses
6	DNS Servers	N/4 DNS server addresses
7	Log Servers	N/4 logging server addresses
8	Cookie Servers	N/4 quote server addresses
9	LPR Servers	N/4 printer server addresses
10	Impress Servers	N/4 impress server addresses
11	RLP Servers	N/4 RLP server addresses
12	Host Name	Hostname string
13	Boot File Size	Size of boot file in 512 byte chunks
14	Merit Dump File	Client to dump and name of file to dump to
15	Domain Name	The DNS domain name of the client
16	Swap Server	Swap server addresses
17	Root Path	Path name for root disk
18	Extension File	Patch name for more BOOTP info
19	IP Layer Forwarding	Enable or disable IP forwarding
20	Src route enabler	Enable or disable source routing
21	Policy Filter	Routing policy filters
22	Maximum DG Reassembly Size	Maximum datagram reassembly size

Option Number	Name	Description
23	Default IP TTL	Default IP time-to-live
24	Path MTU Aging Timeout	Path MTU aging timeout
25	MTU Plateau	Path MTU plateau table
26	Interface MTU Size	Interface MTU size
27	All Subnets Are Local	All subnets are local
28	Broadcast Address	Broadcast address
29	Perform Mask Discovery	Perform mask discovery
30	Provide Mask to Others	Provide mask to others
31	Perform Router Discovery	Perform router discovery
32	Router Solicitation Address	Router solicitation address
33	Static Routing Table	Static routing table
34	Trailer Encapsulation	Trailer encapsulation
35	ARP Cache Timeout	ARP cache timeout
36	Ethernet Encapsulation	Ethernet encapsulation
37	Default TCP Time to Live	Default TCP time to live
38	TCP Keepalive Interval	TCP keepalive interval
39	TCP Keepalive Garbage	TCP keepalive garbage
40	NIS Domain Name	NIS domain name
41	NIS Server Addresses	NIS server addresses
42	NTP Servers Addresses	NTP servers addresses
43	Vendor Specific Information	Vendor specific information
44	NetBIOS Name Server	NetBIOS name server
45	NetBIOS Datagram Distribution	NetBIOS datagram distribution
46	NetBIOS Node Type	NetBIOS node type
47	NetBIOS Scope	NetBIOS scope
48	X Window Font Server	X window font server
49	X Window Display Manager	X window display manager
50	Requested IP address	Requested IP address
51	IP Address Lease Time	IP address lease time
52	Option Overload	Overload "sname" or "file"
53	DHCP Message Type	DHCP message type
54	DHCP Server Identification	DHCP server identification

Option Number	Name	Description
55	Parameter Request List	Parameter request list
56	Message	DHCP error message
57	DHCP Maximum Message Size	DHCP maximum message size
58	Renew Time Value	DHCP renewal (T1) time
59	Rebinding Time Value	DHCP rebinding (T2) time
60	Client Identifier	Client identifier
61	Client Identifier	Client identifier
62	Netware/IP Domain Name	Netware/IP domain name
63	Netware/IP sub Options	Netware/IP sub options
64	NIS+ V3 Client Domain Name	NIS+ V3 client domain name
65	NIS+ V3 Server Address	NIS+ V3 server address
66	TFTP Server Name	TFTP server name
67	Boot File Name	Boot file name
68	Home Agent Addresses	Home agent addresses
69	Simple Mail Server Addresses	Simple mail server addresses
70	Post Office Server Addresses	Post office server addresses
71	Network News Server Addresses	Network news server addresses
72	WWW Server Addresses	WWW server addresses
73	Finger Server Addresses	Finger server addresses
74	Chat Server Addresses	Chat server addresses
75	StreetTalk Server Addresses	StreetTalk server addresses
76	StreetTalk Directory Assistance Addresses	StreetTalk directory assistance addresses
77	User Class Information	User class information
78	SLP Directory Agent	Directory agent information
79	SLP Service Scope	Service location agent scope
80	Rapid Commit	Rapid commit
81	FQDN, Fully Qualified Domain Name	Fully qualified domain name
82	Relay Agent Information	Relay agent information
83	Internet Storage Name Service	Internet storage name service



Option Number	Name	Description
84	Undefined	N/A
85	Novell Directory Servers	Novell Directory Services servers
86	Novell Directory Server Tree Name	Novell Directory Services server tree name
87	Novell Directory Server Context	Novell Directory Services server context
88	BCMCS Controller Domain Name List	CMCS controller domain name list
89	BCMCS Controller IPv4 Address List	BCMCS controller IPv4 address list
90	Authentication	Authentication
91	Undefined	N/A
92	Undefined	N/A
93	Client System	Client system architecture
94	Client Network Device Interface	Client network device interface
95	LDAP Use	Lightweight Directory Access Protocol
96	Undefined	N/A
97	UUID/GUID Based Client Identifier	UUID/GUID-based client identifier
98	Open Group's User Authentication	Open group's user authentication
99	Undefined	N/A
100	Undefined	N/A
101	Undefined	N/A
102	Undefined	N/A
103	Undefined	N/A
104	Undefined	N/A
105	Undefined	N/A
106	Undefined	N/A
107	Undefined	N/A
108	Undefined	N/A
109	Autonomous System Number	Autonomous system number
110	Undefined	
111	Undefined	
112	NetInfo Parent Server Address	NetInfo parent server address
113	NetInfo Parent Server Tag	NetInfo parent server tag
114	URL:	URL

Option Number	Name	Description
115	Undefined	N/A
116	Auto Configure	DHCP auto-configuration
117	Name Service Search	Name service search
118	Subnet Collection	Subnet selection
119	DNS Domain Search List	DNS domain search list
120	SIP Servers DHCP Option	SIP servers DHCP option
121	Classless Static Route Option	Classless static route option
122	CCC, CableLabs Client Configuration	CableLabs client configuration
123	GeoConf	GeoConf
124	Vendor-Identifying Vendor Class	Vendor-identifying vendor class
125	Vendor Identifying Vendor Specific	Vendor-identifying vendor specific
126	Undefined	N/A
127	Undefined	N/A
128	TFTP Server IP Address	TFTP server IP address for IP phone software load
129	Call Server IP Address	Call server IP address
130	Discrimination String	Discrimination string to identify vendor
131	Remote Statistics Server IP Address	Remote statistics server IP address
132	802.1Q VLAN ID	IEEE 802.1Q VLAN ID
133	802.1Q L2 Priority	IEEE 802.1Q layer 2 priority
134	Diffserv Code Point	Diffserv code point for VoIP signalling and media streams
135	HTTP Proxy For Phone Applications	HTTP proxy for phone-specific applications
136	Undefined	N/A
137	Undefined	N/A
138	Undefined	N/A
139	Undefined	N/A
140	Undefined	N/A
141	Undefined	N/A
142	Undefined	N/A
143	Undefined	N/A
144	Undefined	N/A
145	Undefined	N/A
146	Undefined	N/A

Option Number	Name	Description
147	Undefined	N/A
148	Undefined	N/A
149	Undefined	N/A
150	TFTP Server Address, Etherboot, GRUB Config	TFTP server address, Etherboot, GRUB configuration
151	Undefined	
152	Undefined	N/A
153	Undefined	N/A
154	Undefined	N/A
155	Undefined	N/A
156	Undefined	N/A
157	Undefined	N/A
158	Undefined	N/A
159	Undefined	N/A
160	Undefined	N/A
161	Undefined	N/A
162	Undefined	N/A
163	Undefined	N/A
164	Undefined	N/A
165	Undefined	N/A
166	Undefined	N/A
167	Undefined	N/A
168	Undefined	N/A
169	Undefined	N/A
170	Undefined	N/A
171	Undefined	N/A
172	Undefined	N/A
173	Undefined	N/A
174	Undefined	N/A
175	Ether Boot	Ether Boot
176	IP Telephone	IP telephone
177	Ether Boot PacketCable and CableHome	Ether Boot PacketCable and CableHome
178	Undefined	N/A
179	Undefined	N/A
180	Undefined	N/A
181	Undefined	N/A
182	Undefined	N/A

Option Number	Name	Description
183	Undefined	N/A
184	Undefined	N/A
185	Undefined	N/A
186	Undefined	N/A
187	Undefined	N/A
188	Undefined	N/A
189	Undefined	N/A
190	Undefined	N/A
191	Undefined	N/A
192	Undefined	N/A
193	Undefined	N/A
194	Undefined	N/A
195	Undefined	N/A
196	Undefined	N/A
197	Undefined	N/A
198	Undefined	N/A
199	Undefined	N/A
200	Undefined	N/A
201	Undefined	N/A
202	Undefined	N/A
203	Undefined	N/A
204	Undefined	N/A
205	Undefined	N/A
206	Undefined	N/A
207	Undefined	N/A
208	pxelinux.magic (string) = 241.0.116.126	pxelinux.magic (string) = 241.0.116.126
209	pxelinux.configfile (text)	pxelinux.configfile (text)
210	pxelinux.pathprefix (text)	pxelinux.pathprefix (text)
211	pxelinux.reboottime	pxelinux.reboottime
212	Undefined	N/A
213	Undefined	N/A
214	Undefined	N/A
215	Undefined	N/A
216	Undefined	N/A
217	Undefined	N/A
218	Undefined	N/A
219	Undefined	N/A

Option Number	Name	Description
220	Subnet Allocation	Subnet allocation
221	Virtual Subnet Allocation	Virtual subnet selection
222	Undefined	N/A
223	Undefined	N/A
224	Private Use	Private use
225	Private Use	Private use
226	Private Use	Private use
227	Private Use	Private use
228	Private Use	Private use
229	Private Use	Private use
230	Private Use	Private use
231	Private Use	Private use
232	Private Use	Private use
233	Private Use	Private use
234	Private Use	Private use
235	Private Use	Private use
236	Private Use	Private use
237	Private Use	Private use
238	Private Use	Private use
239	Private Use	Private use
240	Private Use	Private use
241	Private Use	Private use
242	Private Use	Private use
243	Private Use	Private use
244	Private Use	Private use
245	Private Use	Private use
246	Private Use	Private use
247	Private Use	Private use
248	Private Use	Private use
249	Private Use	Private use
250	Private Use	Private use
251	Private Use	Private use
252	Private Use	Private use
253	Private Use	Private use
254	Private Use	Private use



# CHAPTER 24

## Using IP Helper

### Network > IP Helper

The IP Helper allows the SonicWALL security appliance to forward DHCP requests originating from the interfaces on a SonicWALL security appliance to a centralized DHCP server on the behalf of the requesting client. IP Helper is used extensively in routed VLAN environments where a DHCP server is not available for each interface, or where the layer 3 routing mechanism is not capable of acting as a DHCP server itself. The IP Helper also allows NetBIOS broadcasts to be forwarded with DHCP client requests. For more information on IP Helper, refer to the IP Helper technote at:

[http://www.sonicwall.com/us/support/2134\\_3424.html](http://www.sonicwall.com/us/support/2134_3424.html)



### IP Helper Settings

- **Enable IP Helper** - enables IP Helper features.
- **Enable DHCP Support** - enables DHCP forwarding from the SonicWALL security appliance to your central DHCP server. If the DHCP server has been enabled, the message “**DHCP Server has been enabled. To edit this setting, click here.**” is displayed. Clicking the link displays the **Network > DHCP Server** page.

**Caution** The SonicWALL DHCP Server feature must be disabled before you can enable DHCP Support on the IP Helper. The **Enable DHCP Support** checkbox is greyed out until the DHCP Server setting is disabled.

- **Enable NetBIOS Support** - enables NetBIOS broadcast forwarding with the DHCP requests. NetBIOS is required to allow Windows operating systems to browse for resources on a network.

## IP Helper Policies

**IP Helper Policies** allow you to forward DHCP and NetBIOS broadcasts from one interface to another interface.

## Adding an IP Helper Policy

- Step 1** Click the **Add** button under the **IP Helper Policies** table. The **Add IP Helper Policy** window is displayed.



- Step 2** The policy is enabled by default. To configure the policy without enabling it, clear the **Enabled** check box.
- Step 3** Select **DHCP** or **NetBIOS** from the **Protocol** menu.
- Step 4** Select a source Interface or Zone from the **From** menu.
- Step 5** Select a destination IP address or subnet from the **To** menu or select **Create a new network** to create a new **Address Object**.
- Step 6** Enter an optional comment in the **Comment** field.
- Step 7** Click **OK** to add the policy to the **IP Helper Policies** table.

## Editing an IP Helper Policy

Click the **Notepad** icon in the **Configure** column of the **IP Helper Policies** table to display the **Edit IP Helper** window, which includes the same settings as the **Add IP Helper Policy** window.

## Deleting IP Helper Policies

Click the Trashcan icon to delete the individual IP Helper policy entry.

Click the **Delete** button to delete all the selected IP Helper policies in the **IP Helper Policies** table.





## CHAPTER 25

# Setting Up Web Proxy Forwarding

---

## Network > Web Proxy

A Web proxy server intercepts HTTP requests and determines if it has stored copies of the requested Web pages. If it does not, the proxy completes the request to the server on the Internet, returning the requested information to the user and also saving it locally for future requests. Setting up a Web proxy server on a network can be cumbersome, because each computer on the network must be configured to direct Web requests to the server.

If you have a proxy server on your network, instead of configuring each computer's Web browser to point to the proxy server, you can move the server to the WAN and enable Web Proxy Forwarding using the settings on the **Network > Web Proxy** page. The SonicWALL security appliance automatically forwards all Web proxy requests to the proxy server without requiring all the computers on the network to be configured.



## Configuring Automatic Proxy Forwarding (Web Only)



**Note**

---

The proxy server must be located on the WAN; it can not be located on the LAN.

---

To configure a Proxy Web sever, select the **Network > Web Proxy** page.

- 
- Step 1** Connect your Web proxy server to a hub, and connect the hub to the SonicWALL security appliance WAN port.
  - Step 2** Type the name or IP address of the proxy server in the **Proxy Web Server (name or IP address)** field.
  - Step 3** Type the proxy IP port in the **Proxy Web Server Port** field.
  - Step 4** To bypass the Proxy Servers if a failure occurs, select the **Bypass Proxy Servers Upon Proxy Server Failure** check box.
  - Step 5** Select **Forward DMZ Client Requests to Proxy Server** if you have clients configured on the DMZ.
  - Step 6** Click **Apply**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the browser window.

## Bypass Proxy Servers Upon Proxy Failure

If a Web proxy server is specified on the **Firewall > Web Proxy** page, selecting the **Bypass Proxy Servers Upon Proxy Server Failure** check box allows clients behind the SonicWALL security appliance to bypass the Web proxy server in the event it becomes unavailable. Instead, the client's browser accesses the Internet directly as if a Web proxy server is not specified.

# CHAPTER 26

## Configuring Dynamic DNS

### Network > Dynamic DNS

Dynamic DNS (DDNS) is a service provided by various companies and organizations that allows for dynamic changing IP addresses to automatically update DNS records without manual intervention. This service allows for network access using domain names rather than IP addresses, even when the target's IP addresses change. For example, if a user has a DSL connection with a dynamically assigned IP address from the ISP, the user can use DDNS to register the IP address, and any subsequent address changes, with a DDNS service provider so that external hosts can reach it using an unchanging domain name.

Dynamic DNS implementations change from one service provider to another. There is no strict standard for the method of communication, for the types of records that can be registered, or for the types of services that can be offered. Some providers offer premium versions of their services, as well, for a fee. As such, supporting a particular DDNS provider requires explicit interoperability with that provider's specific implementation.

Most providers strongly prefer that DDNS records only be updated when IP address changes occur. Frequent updates, particularly when the registered IP address is unchanged, may be considered abuse by providers, and could result in your DDNS account getting locked out. Please refer to the use policies posted on the provider's pages, and abide by the guidelines. SonicWALL does not provide technical support for DDNS providers - the providers themselves must be contacted.

Profile Name	Domain	Provider	Status	Enabled	Online	Configure
DDNS Example	example.sonicwall.com	DynDNS.org		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

### Supported DDNS Providers

Not all services and features from all providers are supported, and the list of supported providers is subject to change. SonicOS currently supports the following services from four Dynamic DNS providers:

- Dyndns.org <http://www.dyndns.org> - SonicOS requires a username, password, Mail Exchanger, and Backup MX to configure DDNS from Dyndns.org.
- Changeip.com <http://www.changeip.com> - A single, traditional Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration.
- No-ip.com <http://www.no-ip.com> - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Also supports hostname grouping.
- Yi.org <http://www.yi.org> - Dynamic DNS service requiring only username, password, and domain name for SonicOS configuration. Requires that an RR record be created on the yi.org administrative page for dynamic updates to occur properly.

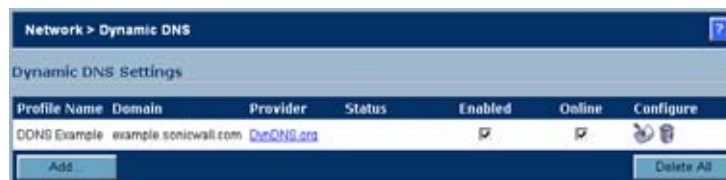
## Additional Services offered by Dynamic DNS Providers

Some common additional services offered by Dynamic DNS providers include:

- **Wildcards** - allows for wildcard references to sub-domains. For example, if you register yourdomain.dyndns.org, your site would be reachable at \*.yourdomain.dyndyn.org, e.g. server.yourdomain.dyndyn.org, www.yourdomain.dyndyn.org, ftp.yourdomain.dyndyn.org, etc.
- **Mail Exchangers** - Creates MX record entries for your domain so that SMTP servers can locate it via DNS and send mail. Note: inbound SMTP is frequently blocked by ISPs - please check with your provider before attempting to host a mail server.
- **Backup MX** (offered by dyndns.org, yi.org) - Allows for the specification of an alternative IP address for the MX record in the event that the primary IP address is inactive.
- **Groups** - Allows for the grouping of hosts so that an update can be performed once at the group level, rather than multiple times for each member.
- **Off-Line IP Address** - Allows for the specification of an alternative address for your registered hostnames in the event that the primary registered IP is offline.

## Configuring Dynamic DNS

Using any Dynamic DNS service begins with settings up an account with the DDNS service provider (or providers) of your choice. It is possible to use multiple providers simultaneously. Refer to the links for the various providers listed above. The registration process normally involves a confirmation email from the provider, with a final acknowledgment performed by visiting a unique URL embedded in the confirmation email. After logging in to the selected provider's page, you should visit the administrative link (typically 'add' or 'manage'), and create your host entries. This must be performed prior to attempting to use the dynamic DNS client on SonicOS. The **Network > Dynamic DNS** page provides the settings for configuring the SonicWALL security appliance to use your DDNS service.



To configure Dynamic DNS on the SonicWALL security appliance, perform these steps:

- Step 1** From the **Network > Dynamic DNS** page, click the **Add** button. The **Add DDNS Profile** window is displayed.

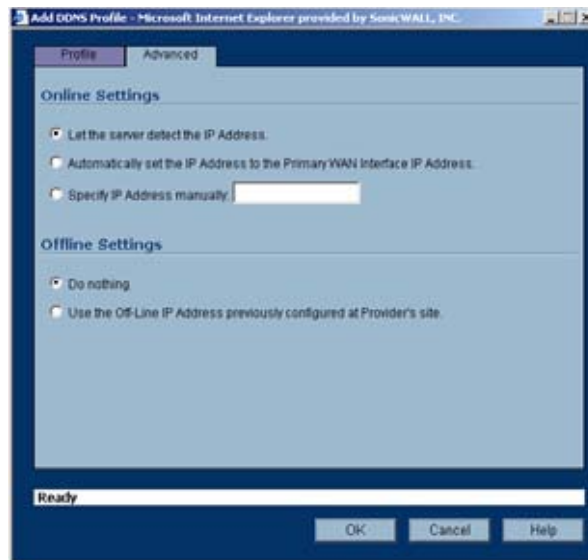


- Step 2** If **Enable this DDNS Profile** is checked, the profile is administratively enabled, and the SonicWALL security appliance takes the actions defined in the **Online Settings** section on the **Advanced** tab.
- Step 3** If **Use Online Settings** is checked, the profile is administratively online.
- Step 4** Enter a name to assign to the DDNS entry in the **Profile Name** field. This can be any value used to identify the entry in the **Dynamic DNS Settings** table.
- Step 5** In the **Profile** page, select the **Provider** from the drop-down list at the top of the page. *DynDNS.org* and *changeip.com* use HTTPS, while *yi.org* and *no-ip.com* use HTTP. This example uses *DynDNS.org*. DynDNS.org requires the selection of a service. This example assumes you have created a dynamic service record with dynDNS.org.
- Step 6** Enter your dynDNS.org username and password in the **User Name** and **Password** fields.
- Step 7** Enter the fully qualified domain name (FQDN) of the hostname you registered with dynDNS.org. Make sure you provide the same hostname and domain as you configured.
- Step 8** When using *DynDNS.org*, select the **Service Type** from the drop-down list that corresponds to your type of service through DynDNS.org. The options are:
- **Dynamic** - A free Dynamic DNS service.
  - **Custom** - A managed primary DNS solution that provides a unified primary/secondary DNS service and a web-based interface. Supports both dynamic and static IP addresses.

- **Static** - A free DNS service for static IP addresses.

**Step 9** When using *DynDNS.org*, you may optionally select **Enable Wildcard** and/or configure an MX entry in the **Mail Exchanger** field. Check **Backup MX** if this is the backup mail exchanger.

**Step 10** Click the **Advanced** tab. You can typically leave the default settings on this page.



**Step 11** The **On-line Settings** section provides control over what address is registered with the dynamic DNS provider. The options are:

- **Let the server detect IP Address** - The dynamic DNS provider determines the IP address based upon the source address of the connection. This is the most common setting.
- **Automatically set IP Address to the Primary WAN Interface IP Address** - This will cause the SonicWALL device to assert its WAN IP address as the registered IP address, overriding auto-detection by the dynamic DNS server. Useful if detection is not working correctly.
- **Specify IP Address manually** - Allows for the IP address to be registered to be manually specified and asserted.

**Step 12** The **Off-line Settings** section controls what IP Address is registered with the dynamic DNS service provider if the dynamic DNS entry is taken off-line locally (disabled) on the SonicWALL. The options are:

- **Do nothing** - the default setting. This allows the previously registered address to remain current with the dynamic DNS provider.
- Use the Off-Line IP Address previously configured at Providers site - If your provider supports manual configuration of Off-Line Settings, you can select this option to use those settings when this profile is taken administratively offline.

**Step 13** Click **OK**.



## Dynamic DNS Settings Table

The **Dynamic DNS Settings** table provides a table view of configured DDNS profiles.

Profile Name	Domain	Provider	Status	Enabled	Offline	Configure
profile2	mcsafe-dns.org	Dyndns.com	Online: 87.110.110.86 at 1/10/2004 11:52:26	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
profile1	mcsafe-dns.org	Dyndns.com	Online: 86.142.80.78 at 1/10/2004 11:21:55	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

**Dynamic DNS Settings** table includes the following columns:

- **Profile Name** - The name assigned to the DDNS entry during its creation. This can be any value, and is used only for identification.
- **Domain** - The fully qualified domain name (FQDN) of the DDNS entry.
- **Provider** - The DDNS provider with whom the entry is registered.
- **Status** - The last reported/current status of the DDNS entry. Possible states are:
  - **Online** - The DDNS entry is administratively online. The current IP setting for this entry is shown with a timestamp.
  - **Taken Offline Locally** - The DDNS entry is administratively offline. If the entry is Enabled, the action configured in the Offline Settings section of the Advanced tab is taken.
  - **Abuse** - The DDNS provider has considered the type or frequency of updates to be abusive. Please check with the DDNS provider's guidelines to determine what is considered abuse.
  - **No IP change** - abuse possible - A forced update without an IP address change is considered by some DDNS providers to be abusive. Automatic updates will only occur when address or state changes occur. Manual or forced should only be made when absolutely necessary, such as when registered information is incorrect.
  - **Disabled** - The account has been disabled because of a configuration error or a policy violation. Check the profile's settings, and verify the DDNS account status with the provider.
  - **Invalid Account** - The account information provided is not valid. Check the profile's settings, and verify the DDNS account status with the provider.
  - **Network Error** - Unable to communicate with the DDNS provider due to a suspected network error. Verify that the provider is reachable and online. Try the action again later.
  - **Provider Error** - The DDNS provider is unable to perform the requested action at this time. Check the profile's settings, and verify the DDNS account status with the provider. Try the action again later.
  - **Not Donator Account** - Certain functions provided from certain provider, such as offline address settings, are only available to paying or donating subscribers. Please check with the provider for more details on which services may require payment or donation.
- **Enabled** - When selected, this profile is administratively enabled, and the SonicWALL will take the **Online Settings** action that is configured on the **Advanced** tab. This setting can also be controlled using the **Enable this DDNS Profile** checkbox in the entry's **Profile** tab. Deselecting this checkbox will disable the profile, and no communications with the DDNS provider will occur for this profile until the profile is again enabled.

- **Online** - When selected, this profile is administratively online. The setting can also be controlled using the **Use Online Settings** checkbox on the entry's **Profile** tab. Deselecting this checkbox while the profile is enabled will take the profile offline, and the SonicWALL will take the **Offline Settings** action that is configured on the **Advanced** tab.
- **Configure** - Includes the edit  icon for configuring the DDNS profile settings, and the delete  icon for deleting the DDNS profile entry.



# **PART 4**

# **Wireless**

•





## CHAPTER 27

# Viewing WLAN Settings, Statistics, and Station Status

---

## Wireless Overview

The SonicWALL Wireless security appliances support two wireless protocols called IEEE 802.11b and 802.11g, commonly known as Wi-Fi, and send data via radio transmissions. The SonicWALL wireless security appliance combines three networking components to offer a fully secure wireless firewall: an Access Point, a secure wireless gateway, and a stateful firewall with flexible NAT and VPN termination and initiation capabilities. With this combination, the wireless security appliance offers the flexibility of wireless without compromising network security.

Typically, the wireless security appliance is the access point for your wireless LAN and serves as the central access point for computers on your LAN. In addition, it shares a single broadband connection with the computers on your network. Since the wireless security appliance also provides firewall protection, intruders from the Internet cannot access the computers or files on your network. This is especially important for an “always-on” connection such as a DSL or T1 line that is shared by computers on a network.

However, wireless LANs are vulnerable to “eavesdropping” by other wireless networks which means you should establish a wireless security policy for your wireless LAN. On the wireless security appliance, wireless clients connect to the Access Point layer of the firewall. Instead of bridging the connection directly to the wired network, wireless traffic is first passed to the Secure Wireless Gateway layer where the client is required to be authenticated via User Level Authentication. Wireless access to Guest Services and MAC Filter Lists are managed by the wireless security appliance. It is also at this layer that the wireless security appliance has the capability of enforcing WiFiSec, an IPsec-based VPN overlay for wireless networking. As wireless network traffic successfully passes through these layers, it is then passed to the VPN-NAT-Stateful firewall layer where WiFiSec termination, address translation, and access rules are applied. If all of the security criteria is met, then wireless network traffic can then pass via one of the following Distribution Systems (DS):

- LAN
- WAN
- Wireless Client on the WLAN
- DMZ or other zone on Opt port

- VPN tunnel

**SONICWALL** COMPREHENSIVE INTERNET SECURITY™

System  
Network  
Modem  
Wireless

Wireless > Status Clear Statistics ?

Access Point 'sonicwall' Status

**WLAN Settings**

- WLAN: **Enabled**
- WiFiSec Enforcement: **Enabled**
- SSID: sonicwall
- MAC Address (BSSID): 00:06:91:12:4D:FC
- WLAN IP Address: 172.16.31.1
- WLAN Subnet Mask: 255.255.255.0
- Regulatory Domain: FCC - North America
- Channel: AutoChannel - Currently Channel 1
- Radio Tx Rate: 54 Mbps
- Radio Tx Power: High
- Authentication Type: **Disabled**
- MAC Filter List: **Disabled**
- Wireless Guest Services: **Disabled**
- Intrusion Detection: **Enabled**
- Wireless Firmware: 1.0.4.3
- Associated Stations: 1 of 32 maximum
- Radio Mode: 2.4GHz 802.11b/g Mixed

**WLAN Statistics**

Wireless Statistics	Bx	Ix
Unicast Frames	31	1006
Multicast Frames	69	70
Fragments	0	0
Total Packets	100	92
Total Bytes	12897	8695
Errors	N/A	4042
Single Retry Frames	N/A	0
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	0
Discards	2151282444	0
Discards: Bad WEP Key	0	N/A
FCS Errors	141991	N/A
Frames Received	1263664	N/A
Frames Aborted	53463	N/A
Frames Aborted Pkty	555285	N/A
Duplicate Frames	0	N/A

**Station Status**

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Configure
1	00:90:4B:76:20:3B	Authenticated	Associated	25	94%	49s	

[Delete All](#)

Status: Ready

## Considerations for Using Wireless Connections

- **Mobility** - if the majority of your network is laptop computers, wireless is more portable than wired connections.
- **Convenience** - wireless networks do not require cabling of individual computers or opening computer cases to install network cards.
- **Speed** - if network speed is important to you, you may want to consider using Ethernet connections rather than wireless connections.
- **Range and Coverage** - if your network environment contains numerous physical barriers or interference factors, wireless networking may not be suitable for your network.
- **Security** - wireless networks have inherent security issues due to the unrestricted nature of the wireless transmissions. However, the wireless security appliance is a firewall and has NAT capabilities which provides security, and you can use WiFiSec to secure data transmissions.

## Recommendations for Optimal Wireless Performance

- Place the wireless security appliance near the center of your intended network. This can also reduce the possibility of eavesdropping by neighboring wireless networks.
- Minimize the number of walls or ceilings between the wireless security appliance and the receiving points such as PCs or laptops.

- Try to place the wireless security appliance in a direct line with other wireless components. Best performance is achieved when wireless components are in direct line of sight with each other.
- Building construction can make a difference on wireless performance. Avoid placing the wireless security appliance near walls, fireplaces, or other large solid objects. Placing the wireless security appliance near metal objects such as computer cases, monitors, and appliances can affect performance of the unit.
- Metal framing, UV window film, concrete or masonry walls, and metallic paint can reduce signal strength if the wireless security appliance is installed near these types of materials.
- Installing the wireless security appliance in a high place can help avoid obstacles and improve performance for upper stories of a building.
- Neighboring wireless networks and devices can affect signal strength, speed, and range of the wireless security appliance. Also, devices such as cordless phones, radios, microwave ovens, and televisions may cause interference on the wireless security appliance.

## Adjusting the Antennas

The antennas on the wireless security appliance can be adjusted for the best radio reception. Begin with the antennas pointing straight up, and then adjust as necessary. Note that certain areas, such as the area directly below the wireless security appliance, get relatively poor reception. Pointing the antenna directly at another wireless device does not improve reception. Do not place the antennas next to metal doors or walls as this can cause interference.

## Wireless Node Count Enforcement

Users connecting to the WLAN or connecting through the SonicWALL GroupVPN are not counted towards the node enforcement on the SonicWALL. Only users on the LAN and non-Wireless zones on the Opt port are counted towards the node limit.

The Station Status table lists all the wireless nodes connected.

## MAC Filter List

The SonicWALL wireless security appliance networking protocol provides native MAC address filtering capabilities. When MAC address filtering is enabled, filtering occurs at the 802.11 layer, wireless clients are prevented from authenticating and associating with the wireless access point. Since data communications cannot occur without authentication and association, access to the network cannot be granted until the client has given the network administrator the MAC address of their wireless network card.

## WiFiSec Enforcement

Enabling **WiFiSec Enforcement** on the wireless security appliance enforces the use of IPsec-based VPN for access from the WLAN to the WAN or LAN, and provides access from the WLAN to the WAN independent of WGS. Access from one wireless client to another is configured on the **Wireless > Advanced** page where you can disable or enable access between wireless clients.

WiFiSec uses the easy provisioning capabilities of the SonicWALL Global VPN client making it easy for experienced and inexperienced administrators to implement on the network. The level of interaction between the Global VPN Client and the user depends on the WiFiSec options selected by the administrator. WiFiSec IPsec terminates on the WLAN/LAN port, and is configured using the Group VPN Security Policy including noneditable parameters specifically for wireless access.

## Wireless > Status

The **Wireless > Status** page provides status information for wireless network, including **WLAN Settings**, **WLAN Statistics**, **WLAN Activities** and **Station Status**.

The screenshot displays the 'Wireless > Status' page for an Access Point 'sonicwall'. It is divided into three main sections: WLAN Settings, WLAN Statistics, and Station Status.

**WLAN Settings:**

- WLAN: Enabled
- WiFiSec Enforcement: Enabled
- SSID: sonicwall
- MAC Address (BSSID): 00:06:B1:12:4D:FC
- WLAN IP Address: 172.16.31.1
- WLAN Subnet Mask: 255.255.255.0
- Regulatory Domain: FCC - North America
- Channel: AutoChannel - Currently Channel 1
- Radio Tx Rate: 54 Mbps
- Radio Tx Power: High
- Authentication Type: Disabled
- MAC Filter List: Disabled
- Wireless Guest Services: Disabled
- Intrusion Detection: Enabled
- Wireless Firmware: 1.0.4.3
- Associated Stations: 1 of 32 maximum
- Radio Mode: 2.4GHz 802.11b/g Mixed

**WLAN Statistics:**

Wireless Statistics	Bx	Ix
Unicast Frames	31	1086
Multicast Frames	69	78
Fragments	0	0
Total Packets	100	82
Total Bytes	12897	6895
Errors	N/A	4042
Single Retry Frames	N/A	0
Multiple Retry Frames	N/A	0
Retry Limit Exceeded	N/A	0
Discards	2151202444	0
Discards: Bad WEP Key	0	N/A
FCS Errors	141991	N/A
Frames Received	1263664	N/A
Frames Aborted	53463	N/A
Frames Aborted Pkty	555205	N/A
Duplicate Frames	0	N/A

**Station Status:**

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Configure
1.	00:90:4B:76:20:3B	Authenticated	Associated	25	94%	40s	

Buttons: Clear Statistics, Delete All

The **Wireless > Status** page has four tables:

- “WLAN Settings” on page 319
- “WLAN Statistics” on page 320
- “WLAN Activities” on page 320
- “Station Status” on page 321

## WLAN Settings

The **WLAN Settings** table lists the configuration information for the built-in radio. All configurable settings in the **WLAN Settings** table are hyperlinks to their respective pages for configuration. Enabled features are displayed in green, and disabled features are displayed in red. Click on a setting to go the page in the Management Interface where you can configure that setting.



WLAN Settings	Value
WLAN	Enabled or Disabled
WiFiSec Enforcement	Enabled or Disabled
SSID	Wireless network identification information
MAC Address (BSSID)	Serial Number of the wireless security appliance
WLAN IP Address	IP address of the WLAN port
WLAN Subnet Mask	Subnet information
Regulatory Domain	<b>FCC - North America</b> for domestic appliances <b>ETSI - Europe</b> for international appliances
Channel	Channel Number selected for transmitting wireless signal
Radio Tx Rate	Network speed in Mbps
Radio Tx Power	Current power level of the radio signal transmission
Authentication Type	Encryption settings for the radio, or Disabled--see the <b>Wireless &gt; WEP/WPA Encryption</b> page
MAC Filter List	Enabled or Disabled
Wireless Guest Services	Enabled or Disabled
Intrusion Detection	Enabled or Disabled
Wireless Firmware	Firmware version on the radio card
Associated Stations	Number of clients associated with the wireless security appliance

WLAN Settings	Value
Radio Mode	Current power level of the radio signal transmission

## WLAN Statistics

The **WLAN Statistics** table lists all of the traffic sent and received through the WLAN. The **Wireless Statistics** column lists the kinds of traffic recorded, the **Rx** column lists received traffic, and the **Tx** column lists transmitted traffic.

Wireless Statistics	Rx/TX
Good Packets	Number of allowed packets received and transmitted.
Bad Packets	Number of packets that were dropped that were received and transmitted.
Good Bytes	Total number of bytes in the good packets.
Management Packets	Number of management packets received and transmitted.
Control Packets	Number of control packets received and transmitted.
Data Packets	Number of data packets received and transmitted.
Duplicate Frames	Number or duplicate frames received.

## WLAN Activities




The **WLAN Activities** table describes the history of wireless clients connecting to the SonicWALL wireless security appliance.

Wireless Activities	Value
Associations	Number of wireless clients that have connected to the wireless security appliance.
Disassociations	Number of wireless clients that have disconnected to the wireless security appliance.
Reassociations	Number of wireless clients that were previously connected that have re-connected.
Authentications	Number of wireless clients that have been authenticated.
Deauthentications	Number of authenticated clients that have disconnected.
Discards Packets	Number of discarded packets.






## Station Status

The **Station Status** table displays information about wireless connections associated with the wireless security appliance.

Station	MAC Address	Authenticated	Associated	AID	Signal	Timeout	Configure
1	00:06:B1:12:4D:FC	Authenticated	Associated	56	0%	60s	  

Delete All

- **Station** - the name of the connection used by the MAC address
- **MAC Address** - the wireless network card MAC address
- **Authenticated** - status of 802.11b authentication
- **Associated** - status of 802.11b association
- **AID** - Association ID, assigned by the security appliance
- **Signal** - strength of the radio signal
- **Timeout** - number of seconds left on the session
- **Configure**
  - ◆  - configure power management on the wireless network card of this station, if enabled.
  - ◆  - block the station from the security appliance and add it to the Deny MAC Filter List.
  - ◆  - dissociate the station from the security appliance.



# CHAPTER 28

## Configuring Wireless Settings

### Wireless > Settings

The **Wireless > Settings** page allows you to configure your wireless settings.

On the **Wireless>Settings** page, you can enable or disable the WLAN port by selecting or clearing the **Enable WLAN** checkbox.

### Wireless Radio Mode

Select either **Access Point** to configure the SonicWALL as the default gateway on your network or select **Wireless Bridge** from the **Radio Role** menu to configure the SonicWALL to act as an intermediary wireless device.



**Note**

WPA support is only available in Access Point Mode. WPA support is not available in Wireless Bridge Mode.

## Wireless Settings

**Enable WLAN Radio:** Check this checkbox to turn the radio on, and enable wireless networking. Click **Apply** in the top right corner of the management interface to have this setting take effect.

**Schedule:** The schedule determines when the radio is on to send and receive data. The default value is **Always on**. The Schedule list displays the schedule objects you create and manage in the **System > Schedule** page. The default choices are:

- Always on
- Work Hours or M-T-W-TH-F 08:00-17:00 (these two options are the same schedules)
- **M-T-W-TH-F 00:00-08:00**
- **After Hours** or **M-T-W-TH-F 17:00-24:00** (these two options are the same schedules)
- **Weekend Hours** or **SA-SU 00:00-24:00** (these two options are the same schedules)

**SSID:** The default value, **sonicwall**, for the SSID can be changed to any alphanumeric value with a maximum of 32 characters.

**Radio Mode:** Select your preferred radio mode from the **Radio Mode** menu. The wireless security appliance supports the following modes:

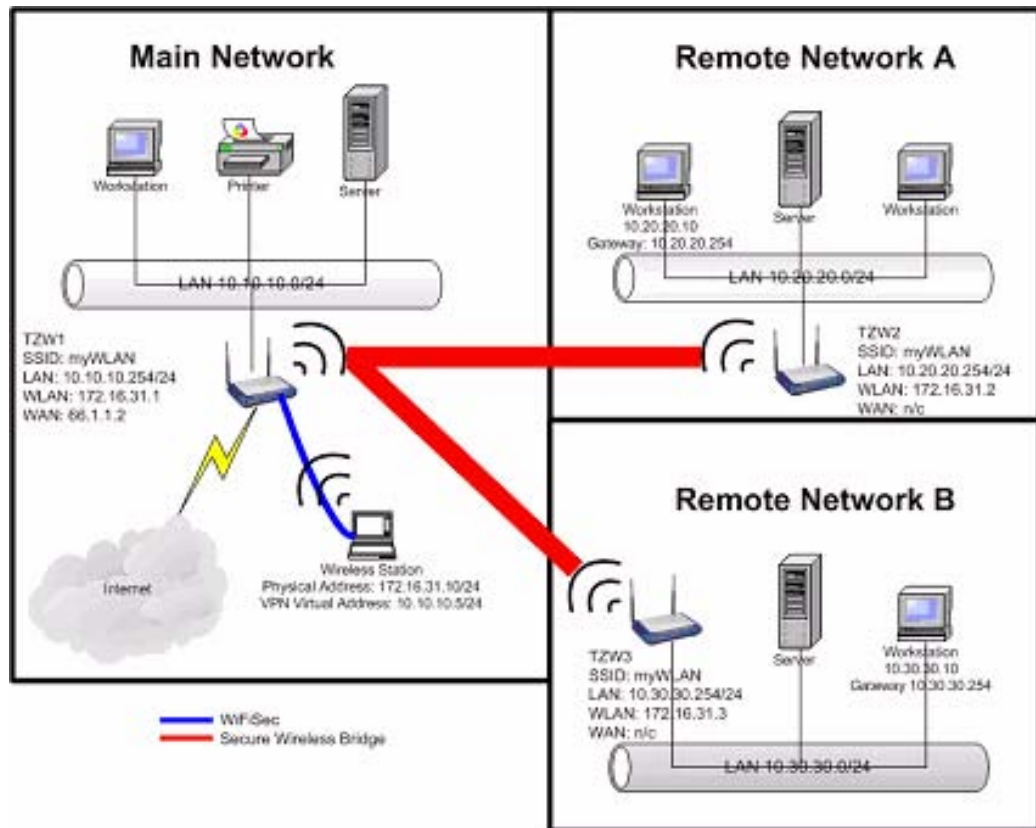
- **2.4GHz 802.11b/g Mixed** - Supports 802.11b and 802.11g clients simultaneously. If your wireless network comprises both types of clients, select this mode.
- **802.11g Only** - If your wireless network consists only of 802.11g clients, you may select this mode for increased 802.11g performance. You may also select this mode if you wish to prevent 802.11b clients from associating.
- **802.11b Only** - Select this mode if only 802.11b clients access your wireless network.

**Channel:** Select the channel for transmitting the wireless signal from the **Channel** menu. An **AutoChannel** setting allows the wireless security appliance to automatically detect and set the optimal channel for wireless operation based upon signal strength and integrity. AutoChannel is the default channel setting, and it displays the selected channel of operation to the right. Alternatively, an operating channel within the range of your regulatory domain can be explicitly defined.

## Secure Wireless Bridging

Wireless Bridging is a feature that allows two or more physically separated networks to be joined over a wireless connection. The wireless security appliance provides this capability by shifting the radio mode at remote networks from **Access Point** mode to **Wireless Bridge**

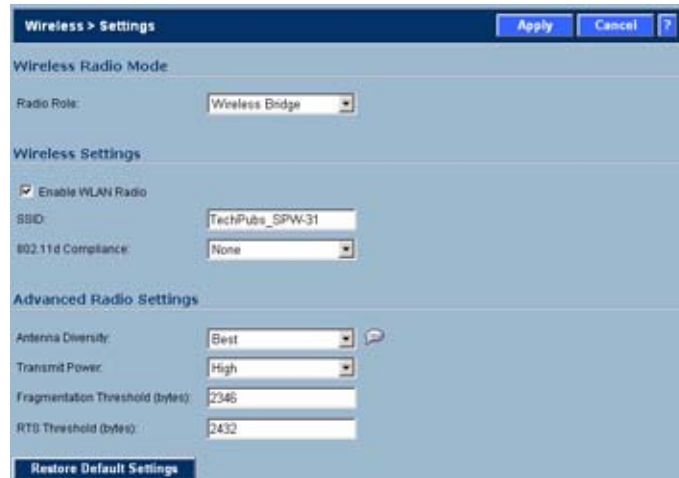
mode. Operating in Wireless Bridge mode, the wireless security appliance connects to another wireless security appliance acting as an access point, and allows communications between the connected networks via the wireless bridge.



Secure Wireless Bridging employs a WiFiSec VPN policy, providing security to all communications between the wireless networks. Previous bridging solutions offered no encryption, or at best, WEP encryption.

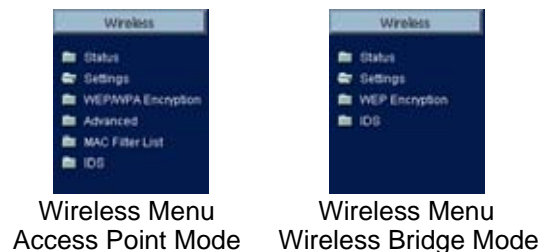
## Configuring a Secure Wireless Bridge


When switching from **Access Point** mode to **Wireless Bridge** mode, all clients are disconnected, and the navigation panel on the left changes to reflect the new mode of operation.



To configure a secure wireless bridge, follow these steps:

- 
- Step 1** Click **Wireless**, then **Settings**.
- Step 2** In the **Wireless Radio Mode** section, select **Wireless Bridge** from the **Radio Role** menu. The wireless security appliance updates the interface. The left-navigation menu changes to reflect the choices that apply to configuring a secure wireless bridge.



- Step 3** In the left-navigation menu, click **Status** under **Wireless**. Any available access point is displayed at the bottom of the **Status** page. Click the **Connect** icon  to establish a wireless bridge to another wireless security appliance.
- Step 4** In the left-navigation menu, click **Settings** under **Wireless**. Configure the WLAN settings for the wireless connection as follows:
- Configure the SSID on all wireless security appliance to the SSID of the Access Point.
  - Configure the WLAN for all wireless security appliance must be on the same subnet.
  - LAN IP address for all wireless security appliance must be on different subnets.

For example, in the previous network diagram, the wireless security appliance are configured as follows:

- SSID on all three wireless security appliance are set to “myWLAN”.
- WLAN addressing for all the wireless security appliance's connected via Wireless Bridge must place the WLAN interfaces on the same subnet: 172.16.31.1 for TZ 170 Wireless1, 172.16.31.2 for TZ 170 Wireless2, and 172.16.31.3 for TZ 170 Wireless3.
- TZ 170 Wireless4 must have a different subnet on the WLAN, such as 172.16.32.X/24.
- LAN addressing for all TZ 170 Wireless connected via Wireless Bridge must place the LAN interfaces on different subnets: 10.10.10.x/24 for TZ 170 Wireless1, 10.20.20.x/24 for TZ 170 Wireless2, and 10.30.30.x/24 for TZ 170 Wireless3.
- LAN addressing for TZ 170 Wireless4 must be the same as TZ 170 Wireless3.
- To facilitate Virtual Adapter addressing, the TZ 170 Wireless4 can be set to forward DHCP requests to TZ 170 Wireless3.
- When a TZ 170 Wireless is in Wireless Bridge mode, the channel cannot be configured. TZ 170 Wireless2 and TZ 170 Wireless3 operate on the channel of the connecting Access Point TZ 170 Wireless. For example, TZ 170 Wireless1 is on channel 1.
- A Bridge Mode TZ 170 Wireless cannot simultaneously support wireless client connections. Access Point services at Remote Site B are provided by a second TZ 170 Wireless (4). The channel of operation is set 5 apart from the channel inherited by the TZ 170 Wireless3. For example, Access Point TZ 170 Wireless1 is set to channel 1, then Bridge Mode TZ 170 Wireless3 inherits channel 1. Access Point TZ 170 Wireless4 should be set to channel 6.

## Network Settings for the Example Network

Device	Mode	SSID	Channel	LAN IP Address	WLAN IP Address
TZ 170 Wireless1	Access Point	myWLAN	1	10.10.10.254/24	172.16.31.1/24
TZ 170 Wireless2	Wireless Bridge	myWLAN	1 (auto)	10.20.20.254/24	172.16.31.2/24
TZ 170 Wireless3	Wireless Bridge	myWLAN	1 (auto)	10.30.30.254/24	172.16.31.3/24
TZ 170 Wireless4	Access Point	otherWLAN	6	10.30.30.253/24	172.16.31.1/24

## Wireless Bridging (without WiFiSec)

To provide compatibility with other non-WiFiSec wireless access points, the wireless security appliance supports a non-secure form of wireless bridging, but insecure wireless communications should only be employed when data is non-sensitive. By default, **WiFiSec Enforcement** is enabled on **Wireless Settings** for **Wireless Bridge Mode**. To connect to a non-WiFiSec access point, this checkbox must be disabled. Since VPN tunnels are not established in non-secure Wireless Bridging deployments, traffic routes must be clearly defined for both the Access Point and the Bridge Mode sites:

- The default route on the Bridge Mode wireless security appliance must from the WLAN interface to the WLAN interface of the connecting Access Point wireless security appliance.

Referring to the example above, the default route on TZ 170 Wireless2 and TZ 170 Wireless3 is set via their WLAN interfaces to 172.16.31.1.

- Static routes must be entered on the Access Point TZ 170 Wireless to route back to the LAN subnets of the Bridge Mode TZ 170 Wireless.

Referring to the example network, TZ 170 Wireless1 must have static routes to 10.20.20.x/24 via 172.16.31.2 and to 10.30.30.x/24 via 172.16.31.3

## Configuring VPN Policies for the Access Point and Wireless Bridge

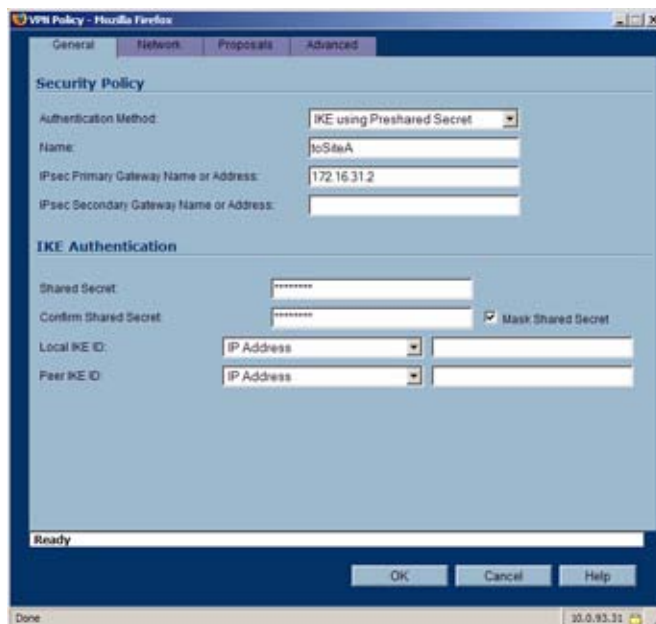
### Access Point Configuration

After Wireless Settings are defined, the WiFiSec connections (VPN Policies) must be configured. The VPN Policies are defined as would any other site-to-site VPN policy, typically with the following in mind:

- The Access Point wireless security appliance must specify the destination networks of the remote sites.
- The Access Point wireless security appliance must specify its LAN management IP address as the **Default LAN Gateway** under the **Advanced** tab.
- The Wireless Bridge Mode wireless security appliance must be configured to use the tunnel as the default route for all internet traffic.

Referring to the example network, the Access Point wireless security appliance has the following two VPN Policies defined:

- One policy to the Site\_A address object at 10.20.20.0:





- One policy to the Site\_B address object at 10.30.30.0:

The screenshot shows the 'VPM Policy - Mozilla Firefox' window with the 'Advanced' tab selected. The 'Security Policy' section is configured as follows:

- Authentication Method: IKE using Preshared Secret
- Name: toSiteB
- IPsec Primary Gateway Name or Address: 172.16.31.2
- IPsec Secondary Gateway Name or Address: (empty)

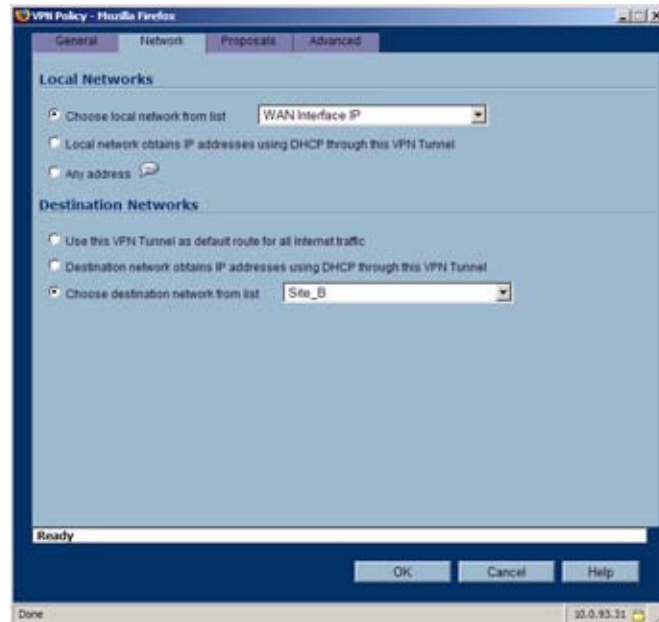
The 'IKE Authentication' section is configured as follows:

- Shared Secret: (masked with asterisks)
- Confirm Shared Secret: (masked with asterisks)
- Mask Shared Secret:
- Local IKE ID: IP Address
- Peer IKE ID: IP Address

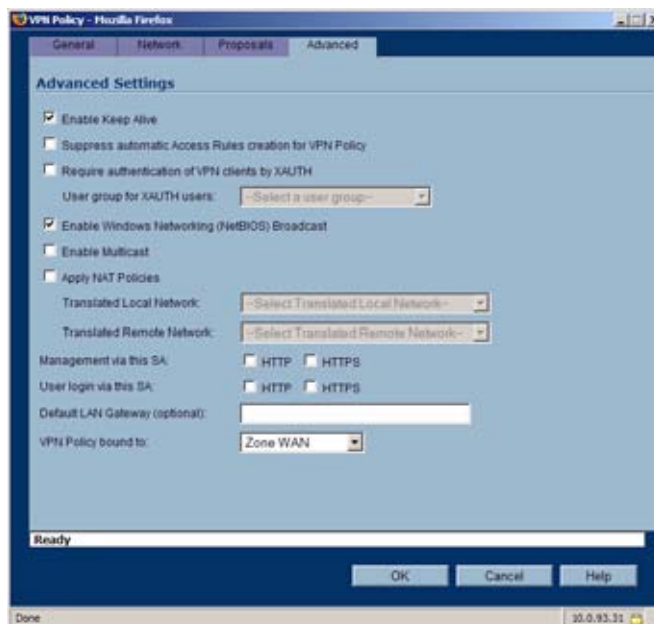
At the bottom of the window, there are 'OK', 'Cancel', and 'Help' buttons. The status bar at the bottom left shows 'Done' and the bottom right shows '30.0.93.31'.

## Configuration for VPN Policies

- Step 1** Click **Network**.
- Step 2** Under **Local Networks**, select **Choose local network from list** and select **LAN Interface IP**.
- Step 3** Under **Destination Networks**, select **Choose destination network from list** and select or create an address object for the destination (Site\_A - 10.20.20.0 or Site\_B - 10.30.30.0 in the example).



- Step 4** Click **Advanced**.
- Step 5** Select **Enable Keep Alive**.
- Step 6** Select **Enable Windows Networking (NetBIOS) Broadcast**.
- Step 7** Click **OK** to close the window, and then click **Apply** for the settings to take effect on the SonicWALL.



### Wireless Bridge VPN Policy Configuration

The Wireless Bridge VPN Policy is configured as follows:

- Step 1** Click **VPN**, then **Configure**.
- Step 2** Select **IKE using Preshared Secret** from the **IPsec Keying Mode** menu.
- Step 3** Enter a name for the SA in the **Name** field.
- Step 4** Type the IP address of the Access Point in the **IPsec Gateway** field. In our example network, the IP address is 172.16.31.1.
- Step 5** Select **Use this VPN Tunnel as default route for all Internet traffic** from the **Destination Networks** section.

Click **OK** to close the window, and then click **Apply** for the settings to take effect on the security appliance.



# CHAPTER 29

## Configuring WEP and WPA Security

### Wireless > WEP/WPA Security



**Note**

When the SonicWALL wireless security appliance is configured in **Access Point** mode, this page is called **Security**. When the appliance is configured in **Wireless Bridge** mode, this page is called **WEP Encryption**.

*Wired Equivalent Protocol* (WEP) can be used to protect data as it is transmitted over the wireless network, but it provides no protection past the SonicWALL. It is designed to provide a minimal level of protection for transmitted data, and is not recommended for network deployments requiring a high degree of security. WiFiSec should be enabled in addition to WEP for added security on the wireless network.

*Wi-Fi Protected Access* (WPA and WPA2) provides much greater security than WEP, but requires a separate authentication protocol, such as RADIUS, be used to authenticate all users. WPA uses a dynamic key that constantly changes, as opposed to the static key that WEP uses.

The SonicWALL Secure Anti-Virus Router provides a number of permutations of WEP and WPA encryption.

**Wireless > Security** [Apply] [Cancel] [?]

**Encryption Mode**

Authentication Type: WPA - EAP

**WPA2/WPA Settings**

Cipher Type:

Group Key Update:

Interval (seconds):

## Authentication Overview

Below is a list of available authentication types with descriptive features and uses for each:

### WEP

- Lower security
- For use with older legacy devices, PDAs, wireless printers

### WPA

- Good security (uses TKIP)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- No client software needed in most cases

### WPA2

- Best security (uses AES)
- For use with trusted corporate wireless clients
- Transparent authentication with Windows log-in
- Client software install may be necessary in some cases
- Supports 802.11i "Fast Roaming" feature
- No backend authentication needed after first log-in (allows for faster roaming)

### WPA2-AUTO

- Tries to connect using WPA2 security.
- If the client is not WPA2 capable, the connection will default to WPA.

## WEP Encryption Settings

**Open-system** authentication is the only method required by 802.11b. In open-system authentication, the SonicWALL allows the wireless client access without verifying its identity.

**Shared-key** authentication uses WEP and requires a shared key to be distributed to wireless clients before authentication is allowed.

The Secure Anti-Virus Router 80 Wireless provides the option of using **Open System**, **Shared Key**, or both when WEP is used to encrypt data.

If **Both (Open System & Shared Key)** is selected, the **Default Key** assignments are not important as long as the identical keys are used in each field. If **Shared Key** is selected, then the key assignment is important.

To configure WEP on the SonicWALL, log into the SonicWALL and click **Wireless**, then **WEP Encryption**.

- 
- Step 1** Select the authentication type from the **Authentication Type** list. **Both (Open System & Shared Key)** is selected by default.
- Step 2** Select 64-bit or 128-bit from the **WEP Key Mode**. 128-bit is considered more secure than 64-bit. This value is applied to all keys.

## WEP Encryption Keys

**Step 1** Select the key number, 1,2,3, or 4, from the **Default Key** menu.

**Step 2** Select the key type to be either **Alphanumeric** or **Hexadecimal**.

WEP - 64-bit	WEP - 128-bit
Alphanumeric - 5 characters (0-9, A-Z)	Alphanumeric - 13 characters (0-9, A-Z)
Hexadecimal - 10 characters (0-9, A-F)	Hexadecimal - 26 characters (0-9, A-F)

**Step 3** Type your keys into each field.

**Step 4** Click **Apply**.

## WPA Encryption Settings

Both WPA and WPA2 support two protocols for storing and generating keys:

- *Pre-Shared Key (PSK)*: PSK allows WPA to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.
- *Extensible Authentication Protocol (EAP)*: EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.

WPA2 also supports EAP and PSK protocols, but adds an optional AUTO mode for each protocol. WPA2 EAP AUTO and WPA2 PSK AUTO try to connect using WPA2 security, but will default back to WPA if the client is not WPA2 capable.



**Note**

WPA support is only available in Access Point Mode. WPA support is not available in Bridge Mode.

## WPA-PSK Settings

The screenshot shows the 'Wireless > Security' configuration window. The 'Authentication Type' is set to 'WPA-PSK'. Under 'WPA2/WPA Settings', the 'Cipher Type' is 'TKIP', 'Group Key Update' is 'By Timeout', and 'Interval (seconds)' is '3600'. Under 'Preshared Key Settings (PSK)', there is a text field for the 'Passphrase'.

**Encryption Mode:** In the **Authentication Type** field, select **WPA-PSK**.

### WPA Settings

- **Cypher Type:** select TKIP. *Temporal Key Integrity Protocol (TKIP)* is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update:** Specifies when the SonicWALL Secure Anti-Virus Router 80 Wireless updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.

### Preshared Key Settings (PSK)

- **Passphrase:** Enter the passphrase from which the key is generated.

Click **Apply** in the top right corner to apply your WPA settings.

## WPA-EAP Settings

The screenshot shows the 'Wireless > Security' configuration window. The 'Authentication Type' is set to 'WPA-EAP'. Under 'WPA2/WPA Settings', the 'Cipher Type' is 'TKIP', 'Group Key Update' is 'By Timeout', and the 'Interval (seconds)' is '3600'. Under 'Extensible Authentication Protocol Settings (EAP)', there are fields for 'Radius Server 1 IP', 'Port', 'Radius Server 1 Secret', 'Radius Server 2 IP', 'Port', and 'Radius Server 2 Secret'.

**Encryption Mode:** In the **Authentication Type** field, select **WPA-EAP**.

### WPA Settings

- **Cypher Type:** Select TKIP. *Temporal Key Integrity Protocol (TKIP)* is a protocol for enforcing key integrity on a per-packet basis.
- **Group Key Update:** Specifies when the SonicWALL Secure Anti-Virus Router 80 Wireless updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA automatically generates a new group key.
- **Packet Threshold:** If you selected **By Packet**, select the number (x 1000) of packets to pass before generating a new group key.

### Extensible Authentication Protocol Settings (EAP)

- **Radius Server 1 IP and Port:** Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret:** Enter the password for access to Radius Server



- **Radius Server 2 IP and Port:** Enter the IP address and port number for your secondary RADIUS server, if you have one.
  - **Radius Server 2 Secret:** Enter the password for access to Radius Server
- Click **Apply** in the top right corner to apply your WPA settings.

## WPA/WPA2 Encryption Settings

Like WPA, WPA2 supports two protocols for storing and generating keys:

- *Pre-Shared Key (PSK):* PSK allows WPA2 to generate keys from a pre-shared passphrase that you configure. The keys are updated periodically based on time or number of packets. Use PSK in smaller deployments where you do not have a RADIUS server.
- *Extensible Authentication Protocol (EAP):* EAP allows WPA to synchronize keys with an external RADIUS server. The keys are updated periodically based on time or number of packets. Use EAP in larger, enterprise-like deployments where you have an existing RADIUS framework.
- *WPA2 PSK / WPA2 EAP:* There are optional AUTO modes for each WPA2 protocol. WPA2 EAP AUTO and WPA2 PSK AUTO try to connect using WPA2 security, and will default back to WPA if the client is not WPA2 capable.



**Note**

WPA2 support is only available in Access Point Mode. WPA support is not available in Bridge Mode.

## WPA2-PSK Settings

The screenshot shows the 'Wireless > Security' configuration window. The 'Authentication Type' is set to 'WPA-PSK'. Under 'WPA2/WPA Settings', the 'Cipher Type' is set to 'TKIP', 'Group Key Update' is set to 'By Timeout', and the 'Interval (seconds)' is set to '3600'. Under 'Preshared Key Settings (PSK)', there is a text field for the 'Passphrase'.

**Encryption Mode:** In the **Authentication Type** field, select **WPA2-PSK**.

**WPA Settings:**

- **Cypher Type:** select AES. *Advanced Encryption Standard (AES)* is an advanced block cipher protocol for enforcing key integrity.
- **Group Key Update:** Specifies when the SonicWALL Secure Anti-Virus Router 80 Wireless updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA2 automatically generates a new group key.

**Preshared Key Settings (PSK)**

- **Passphrase:** Enter the passphrase from which the key is generated.

Click **Apply** in the top right corner to apply your WPA2 settings.

**WPA2-EAP Settings**

The screenshot shows the 'Wireless > Security' configuration window. The 'Encryption Mode' section has 'Authentication Type' set to 'WPA - EAP'. The 'WPA2/WPA Settings' section includes 'Cipher Type' set to 'TKIP', 'Group Key Update' set to 'By Timeout', and 'Interval (seconds)' set to '36400'. The 'Extensible Authentication Protocol Settings (EAP)' section contains fields for 'Radius Server 1 IP', 'Port', 'Radius Server 1 Secret', 'Radius Server 2 IP', 'Port', and 'Radius Server 2 Secret'.

**Encryption Mode:** In the **Authentication Type** field, select **WPA-EAP**.

**WPA Settings**

- **Cypher Type:** select AES. *Advanced Encryption Standard (AES)* is an advanced block cipher protocol for enforcing key integrity.
- **Group Key Update:** Specifies when the SonicWALL Secure Anti-Virus Router 80 Wireless updates the key. Select **By Timeout** to generate a new group key after an interval specified in seconds. Select **By Packet** to generate a new group key after a specific number of packets. Select **Disabled** to use a static key.
- **Interval:** If you selected **By Timeout**, enter the number of seconds before WPA2 automatically generates a new group key.
- **Packet Threshold:** If you selected **By Packet**, select the number (x 1000) of packets to pass before generating a new group key.

**Extensible Authentication Protocol Settings (EAS)**

- **Radius Server 1 IP** and **Port:** Enter the IP address and port number for your primary RADIUS server.
- **Radius Server 1 Secret:** Enter the password for access to Radius Server
- **Radius Server 2 IP** and **Port:** Enter the IP address and port number for your secondary RADIUS server, if you have one.
- **Radius Server 2 Secret:** Enter the password for access to Radius Server

Click **Apply** in the top right corner to apply your WPA2 settings.

# CHAPTER 30

## Configuring Advanced Wireless Settings

### Wireless > Advanced

To access Advanced configuration settings for the SonicWALL wireless security appliance, log into the SonicWALL, click **Wireless**, and then **Advanced**. The **Wireless > Advanced** page is only available when the SonicWALL is acting as an access point.



## Beaconing & SSID Controls

1. Select **Hide SSID in Beacon**. Suppresses broadcasting of the SSID name and disables responses to probe requests. Checking this option helps prevent your wireless SSID from being seen by unauthorized wireless clients.
2. Type a value in milliseconds for the **Beacon Interval**. Decreasing the interval time makes passive scanning more reliable and faster because Beacon frames announce the network to the wireless connection more frequently.

## Wireless Client Communications

1. Enter the number of clients to associate with the SonicWALL wireless security appliance in the **Maximum Client Associations** field. The default value is **32** which means 32 users can access the WLAN at the same time. However, an unlimited number of wireless clients can access the WLAN because node licensing does not apply to the WLAN.
2. If you do not want wireless clients communicating to each other, select **Disabled** from the **Interclient Communications** menu. If you want wireless clients communicating with each other, select **Enabled**. Enabling and disabling Interclient communications changes the associated network access rule on the **Firewall > Access Rules** page.
3. Guests on the wireless network can download the SonicWALL Global VPN Client to install on their computer or laptop. Type the URL location for the software in the **VPN Client Download URL http** field. This field can contain up to 128 characters.

## Configurable Antenna Diversity

The TZ 170 Wireless, TZ 180 Wireless, and TZ 190 Wireless employ dual 5 dBi antennas running in diversity mode. The default implementation of diversity mode means that one antenna acts as a transmitting, and both antennas act as potential receiving antenna. As radio signals arrive at both antennas on the secure wireless appliance, the strength and integrity of the signals are evaluated, and the best received signal is used. The selection process between the two antennas is constant during operation to always provide the best possible signal. To allow for external (higher gain uni-directional) antennas to be used, antenna diversity can be disabled.

The **Antenna Diversity** setting determines which antenna the wireless security appliance uses to send and receive data. You can select:

- **Best**: This is the default setting. When **Best** is selected, the wireless security appliance automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
- **1**: Select **1** to restrict the wireless security appliance to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the console port. You can disconnect antenna 2 when using only antenna 1.

- **2**: Select **2** to restrict the wireless security appliance to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the power supply. You can disconnect antenna 1 when using only antenna 2.



## Advanced Radio Settings

The following other advanced settings can be configured.

**Advanced Radio Settings**

Enable Short Slot Time

Antenna Rx Diversity: Best

Transmit Power: Minimum

Preamble Length: Long

Fragmentation Threshold (bytes): 2346

RTS Threshold (bytes): 2346

DTIM Interval: 1

Association Timeout (seconds): 300

Maximum Client Associations: 32

Data Rate: Best

Protection Mode: Auto

Protection Rate: 11 Mbps

Protection Type: CTS-only

CCK OFDM Power Delta: 1 dBm

**Restore Default Settings**

- Step 1 Enable Short Slot Time:** Select **Enable Short Slot Time** to increase performance if you only expect 802.11g traffic. 802.11b is not compatible with short slot time.
- Step 2** Select **High** from the **Transmit Power** menu to send the strongest signal on the WLAN. For example, select **High** if the signal is going from building-to-building. **Medium** is recommended for office-to-office within a building, and **Low** or **Lowest** is recommended for shorter distance communications.
- Step 3** Select **Short** or **Long** from the **Preamble Length** menu. **Short** is recommended for efficiency and improved throughput on the wireless network.
- Step 4** The **Fragmentation Threshold (bytes)** is 2346 by default. Increasing the value means that frames are delivered with less overhead but a lost or damaged frame must be discarded and retransmitted.
- Step 5** The **RTS Threshold (bytes)** is 2432 by default. If network throughput is slow or a large number of frame retransmissions is occurring, decrease the RTS threshold to enable RTS clearing.
- Step 6** The default value for the **DTIM Interval** is 3. Increasing the DTIM Interval value allows you to conserve power more effectively.
- Step 7** The **Association Timeout (seconds)** is 300 seconds by default. If your network is very busy, you can increase the timeout by increasing the number of seconds in the **Association Timeout (seconds)** field.
- Step 8** Set the **Maximum Client Associations** to limit the number of stations that can connect wirelessly at one time. The default is 32.
- Step 9 Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. You can select: **Best, 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, or 54 Mbps.**
- Step 10 Protection Mode:** Protection can decrease collisions, particularly where you have two

overlapping SonicPoints. However, it can slow down performance. **Auto** is probably the best setting, as it will engage only in the case of overlapping SonicPoints.

- Step 11 Protection Rate:** The protection rate determines the data rate when protection is on. The slowest rate offers the greatest degree of protection but the slowest data transmission rate. Choose **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.
- Step 12 Protection Type:** Select the type of handshake used to establish a wireless connection: **CTS-only** or **RTS-CTS**. 802.11b traffic is only compatible with **CTS**.
- Step 13 CCK OFDM Power Delta:** This setting determines the difference in transmission power between 802.11b (CCK mode) and 802.11g (OFDM mode). When both 802.11g and 802.11b are used simultaneously, 802.11g covers a smaller physical area than 802.11b. Increasing the CCK OFDM Power Delta lowers the transmission power for 802.11b, so the two radio modes will cover the same area. Choose **0 dBm**, **1 dBm**, or **2 dBm**.
- Step 14** Click **Apply** in the top right corner of the page to apply your changes to the security appliance. Click **Restore Default Settings** to return the radio settings to the default settings.





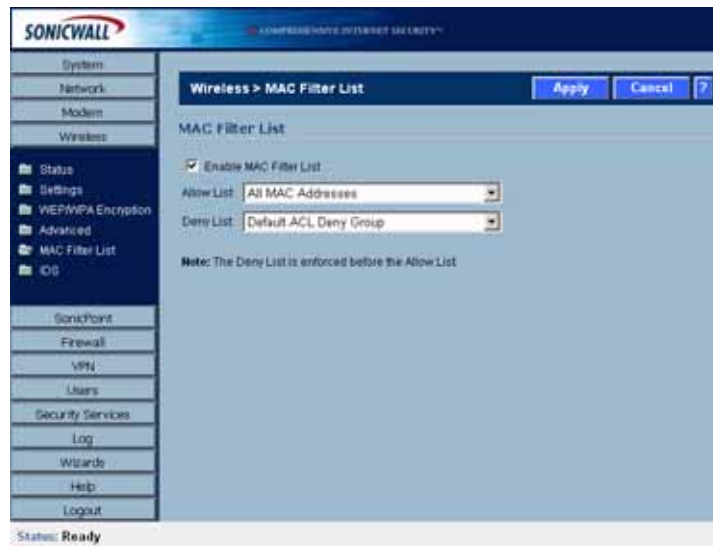
## CHAPTER 31

# Configuring MAC Filter List

## Wireless > MAC Filter List

Wireless networking provides native MAC filtering capabilities which prevents wireless clients from authenticating and associating with the wireless security appliance. If you enforce MAC filtering on the WLAN, wireless clients must provide you with the MAC address of their wireless networking card.

To set up your MAC Filter List, log into the SonicWALL, and click **Wireless**, then **MAC Filter List**.



## Allow or Deny Specific Resources

The MAC **Allow List** contains groups of address objects for network resources that the security appliance allows to connect via the WLAN, regardless of the selections in the deny list.

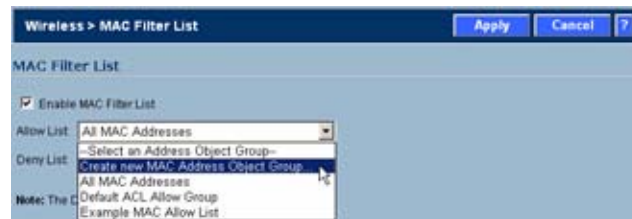
The MAC **Deny List** contains groups of address objects for network resources that the security appliance denies to connect via the WLAN, regardless of the selections in the deny list.

The items in the list are address object groups, defined groups of objects that represent specific IP addresses or ranges of addresses that can be used throughout the management interface to specify network resources. An address object group can contain other address object groups.

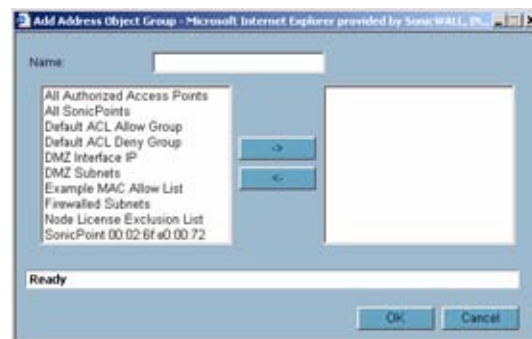
The Allow List and Deny List are also address object groups.

You can create individual objects in the **Wireless > Mac Filter List** page:

- Step 1** In the **Allow List** or **Deny List** box, select Create New MAC Address Object Group.



- Step 2** In the **Add Address Object Group** field, enter a name for the new group
- Step 3** In the left column, select the groups or individual address objects you want to allow or deny. You can use **Ctrl-click** select more than one item.
- Step 4** Click the > button to add the items to the group.



- Step 5** Click **OK** to create the group and add it to the **Allow List** or **Deny List**.

# CHAPTER 32

## Configuring Wireless IDS

### Wireless > IDS

Wireless Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWALL wireless security appliances by enabling them to recognize and even take countermeasures against the most common types of illicit wireless activity. WIDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. Wireless IDS logging and notification can be enabled under **Log > Categories** by selecting the **WLAN IDS** checkbox under **Log Categories** and **Alerts**.

### Wireless Bridge IDS

When the **Radio Role** of the wireless security appliance is set to a Wireless Bridge mode, Rogue Access Point Detection defaults to active mode (actively scanning for other Access Points using probes on all channels).

MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
00:06:B1:12:4B:A1	TechPubs_TZ170W	1	SonicWALL	100 - Excellent	54 Mbps	
00:40:10:56:60:29	dtelehow	1	SonicWALL	80 - Excellent	11 Mbps	
00:02:8F:2E:21:34	voip1	1	Senao	75 - Very good	54 Mbps	
00:06:B1:12:4C:F7	dwpwall-one	1	SonicWALL	70 - Very good	54 Mbps	
00:50:E8:02:05:8E	VSI-BC	1	Unknown	70 - Very good	54 Mbps	
00:06:B1:12:4C:11	local_tz170w_102	1	SonicWALL	80 - Excellent	54 Mbps	
00:06:B1:13:5A:89	sonicwall	1	SonicWALL	78 - Very good	54 Mbps	
00:02:8F:2E:21:FA	sp0	1	Senao	83 - Excellent	54 Mbps	

## Access Point IDS

When the **Radio Role** of the wireless security appliance is set to **Access Point** mode, all three types of WIDS services are available, but Rogue Access Point detection, by default, acts in a passive mode (passively listening to other Access Point Beacon frames only on the selected channel of operation). Selecting **Scan Now** momentarily changes the Radio Role to allow the wireless security appliance to perform an active scan, and may cause a brief loss of connectivity for associated wireless clients. While in **Access Point** mode, the **Scan Now** function should only be used if no clients are actively associated, or if the possibility of client interruption is acceptable.

MAC Address (BSSID)	SSID	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
00:02:6F:2E:20:C4	sonicwall	3	Senao	79 - Very good	54 Mbps	
00:06:B1:12:4C:20	sonicwall	1	SonicWALL	89 - Excellent	54 Mbps	
00:06:B1:12:4D:F0	sonicwall	4	SonicWALL	78 - Very good	54 Mbps	
00:02:6F:2E:20:F8	sonicwall	3	Senao	78 - Very good	54 Mbps	
00:02:6F:2E:21:CC	sonicwall	1	Senao	81 - Excellent	54 Mbps	
00:06:B1:12:71:6B	SHBETA	1	SonicWALL	75 - Very good	54 Mbps	

## Enable Client Null Probing

Enabling this setting allows the wireless security appliance to detect and log Null Probes, such as those used by Netstumbler and other similar tools.

## Association Flood Detection

Association Flood is a type of Wireless Denial of Service attack intended to interrupt wireless services by depleting the resources of a wireless Access Point. An attacker can employ a variety of tools to establish associations, and consequently association IDs, with an access point until it reaches its association limit (generally set to 255). Once association saturation occurs, the access point discards further association attempts until existing associations are terminated.

Association Flood Detection allows thresholds to be set limiting the number of association attempts a client makes in a given span of time before its activities are considered hostile. Association attempts default to a value of 5 (minimum value is 1, maximum value is 100) within and the time period defaults to a value of 5 seconds (minimum value is 1 second, maximum value is 999 seconds). If association attempts exceed the set thresholds, an event is logged according to log settings.

If the **Block station's MAC address in response to an association flood** option is selected and MAC Filtering is enabled, then in addition to logging actions, the wireless security appliance takes the countermeasure of dynamically adding the MAC address to the MAC filter list. Any future Denial of Service attempts by the attacker are then blocked.

**Enable Association Flood Detection** is selected by default. The **Association Flood Threshold** is set to **5 Association attempts within 5 seconds** by default.

## Intrusion Detection Settings

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a and 802.11g channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.


**Enable Rouge Access Point Detection** is enabled by default. The **Authorized Access Points** menu allows you to specify **All Authorized Access Points**, **Create new MAC Address Object Group**, or **Select an Address Object Group**.

The **Authorized Access Points** menu allows you to specify which access points the SonicWALL security appliance will considered authorized when it performs a scan. You can select **All Authorized Access Points** to allow all SonicPoints, or you can select **Create new MAC Address Object Group** to create an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.

Select **Create Address Object Group** to add a new group of MAC address objects to the list.

## Discovered Access Points

The **Discovered Access Points** table displays information on every access point that can be detected by all your SonicPoints or on a individual SonicPoint basis:

- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. SonicPoints will show a manufacturer of either SonicWALL or Senao.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the icon  in the **Authorize** column to add the access point to the address object group of authorized access points.

## Scanning for Access Points

Active scanning occurs when the wireless security appliance starts up, and at any time **Scan Now** is clicked at the bottom of the **Discovered Access Points** table. When the wireless security appliance is operating in a Bridge Mode, the **Scan Now** feature does not cause any interruption to the bridged connectivity. When the wireless security appliance is operating in Access Point Mode, however, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:


- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

---

**Caution** The **Scan Now** feature causes a brief disruption in service. If this is a concern, wait and use the **Scan Now** feature at a time when no clients are active, or the potential for disruption becomes acceptable.

---

## Authorizing Access Points on Your Network

Access Points detected by the wireless security appliance are regarded as rogues until they are identified to the wireless security appliance as authorized for operation. To authorize an access point, select it in the list of access points discovered by the wireless security appliance scanning feature, and add it clicking the **Authorize** icon .



## CHAPTER 33

# Configuring Virtual Access Points

---

## Wireless > Virtual Access Point

This chapter describes the Virtual Access Point feature and includes the following sections:

- [“SonicPoint VAP Overview” section on page 352](#)
  - [“What Is a Virtual Access Point?” section on page 352](#)
  - [“What Is an SSID?” section on page 352](#)
  - [“Wireless Roaming with ESSID” section on page 353](#)
  - [“What Is a BSSID?” section on page 353](#)
  - [“Benefits of Using Virtual APs” section on page 353](#)
- [“Virtual AP Configuration Task List” section on page 353](#)
  - [“VAP Configuration Overview” section on page 354](#)
  - [“Network Zones” section on page 354](#)
  - [“WLAN Subnets” section on page 359](#)
  - [“DHCP Server Scope” section on page 360](#)
  - [“Virtual Access Points Profiles” section on page 361](#)
  - [“Virtual Access Points” section on page 363](#)
  - [“Virtual Access Point Groups” section on page 364](#)
- [“Thinking Critically About VAPs” section on page 365](#)
  - [“Determining Your VAP Needs” section on page 365](#)
  - [“A Sample Network” section on page 365](#)
  - [“Determining Security Configurations” section on page 366](#)
  - [“VAP Configuration Worksheet” section on page 366](#)

## SonicPoint VAP Overview

This section provides an introduction to the Virtual Access Point feature. This section contains the following subsections:

- [“What Is a Virtual Access Point?” section on page 352](#)
- [“What Is an SSID?” section on page 352](#)
- [“Wireless Roaming with ESSID” section on page 353](#)
- [“What Is a BSSID?” section on page 353](#)
- [“Benefits of Using Virtual APs” section on page 353](#)

### What Is a Virtual Access Point?

A Virtual Access Point is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when in actuality there is only a single physical AP. Before the evolution of the Virtual AP feature support, wireless networks were relegated to a one-to-one relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. In other words, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients, and if the latter were required, they would had to have been provided by a separate, distinctly configured Access Points. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows for segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously.

### What Is an SSID?

A Service Set Identifier (SSID) is the name assigned to a wireless network. Wireless clients must use this same, case-sensitive SSID to communicate to the SonicPoint. The SSID consists of a text string up to 32 bytes long. Multiple SonicPoints on a network can use the same SSIDs. You can configure up to 8 unique SSIDs on SonicPoints and assign different configuration settings to each SSID.

SonicPoints broadcast a beacon (announcements of availability of a wireless network) for every SSID configured. By default, the SSID is included within the beacon so that wireless clients can see the wireless networks. The option to suppress the SSID within the beacon is provided on a per-SSID (e.g. per-VAP or per-AP) basis to help conceal the presence of a wireless network, while still allowing clients to connect by manually specifying the SSID.

The following settings can be assigned to each VAP:

- Authentication method
- Maximum number of client associations using the SSID
- SSID Suppression



## Wireless Roaming with ESSID

An ESSID (Extended Service Set Identifier) is a collection of Access Points (or Virtual Access Points) sharing the same SSID. A typical wireless network comprises more than one AP for the purpose of covering geographic areas larger than can be serviced by a single AP. As clients move through the wireless network, the strength of their wireless connection decreases as they move away from one Access Point (AP1) and increases as they move toward another (AP2). Providing AP1 and AP2 are on the same ESSID (for example, 'sonicwall') and that the (V)APs share the same SSID and security configurations, the client will be able to roam from one to the other. This roaming process is controlled by the wireless client hardware and driver, so roaming behavior can differ from one client to the next, but it is generally dependent upon the signal strength of each AP within an ESSID.

## What Is a BSSID?

A BSSID (Basic Service Set Identifier) is the wireless equivalent of a MAC (Media Access Control) address, or a unique hardware address of an AP or VAP for the purposes of identification. Continuing the example of the roaming wireless client from the ESSID section above, as the client on the 'sonicwall' ESSID moves away from AP1 and toward AP2, the strength of the signal from the former will decrease while the latter increases. The client's wireless card and driver constantly monitors these levels, differentiating between the (V)APs by their BSSID. When the card/driver's criteria for roaming are met, the client will detach from the BSSID of AP1 and attach to the BSSID of AP2, all the while remaining connected the 'sonicwall' ESSID.

## Benefits of Using Virtual APs

This section includes a list of benefits in using the Virtual AP feature:

- **Radio Channel Conservation**—Prevents building overlapped infrastructures by allowing a single Physical Access Point to be used for multiple purposes to avoid channel collision problem. Channel conservation. Multiple providers are becoming the norm within public spaces such as airports. Within an airport, it might be necessary to support an FAA network, one or more airline networks, and perhaps one or more Wireless ISPs. However, in the US and Europe, 802.11b networks can only support three usable (non-overlapping) channels, and in France and Japan only one channel is available. Once the channels are utilized by existing APs, additional APs will interfere with each other and reduce performance. By allowing a single network to be used for multiple purposes, Virtual APs conserve channels.

## Virtual AP Configuration Task List

A VAP deployment requires several steps to configure. The following section provides first a brief overview of the steps involved, and then a more in-depth examination of the parts that make up a successful VAP deployment. This subsequent sections describe VAP deployment requirements and provides an administrator configuration task list:

- [“VAP Configuration Overview” section on page 354](#)
- [“Network Zones” section on page 354](#)
- [“WLAN Subnets” section on page 359](#)
- [“DHCP Server Scope” section on page 360](#)
- [“Virtual Access Points Profiles” section on page 361](#)

- [“Virtual Access Points” section on page 363](#)
- [“Virtual Access Point Groups” section on page 364](#)

## VAP Configuration Overview

The following are required areas of configuration for VAP deployment. This sequence of steps is designed specifically to honor dependencies, provide configuration task efficiency, and minimize the total number of required steps for VAP configuration.

1. **Zone** - The Zone is the backbone of your VAP configuration. Each Zone you create will have its own security and access control settings and you can create and apply multiple zones to a single physical interface by way of wireless sub-interfaces.
2. **Wireless Subnet** - The Wireless subnet represents the IP address segment that will be used for the VAP. Each VAP must have its own WLAN subnet, and the WLAN subnet must be created before the VAP is created.
3. **NSA DHCP Server** - The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. It is important to note here that the default ranges for DHCP scopes are often excessive for the needs of most NSA wireless appliance deployments. For instance, a scope of 200 addresses for a sub-interface that only supports 30 users is rather excessive. Be aware of this during your setup and take care to ensure the available DHCP lease scope for your NSA is not exhausted.
4. **Virtual Access Points** - The Virtual Access Points section allows for setup of general VAP settings including SSID, wireless subnet association and authentication settings.
5. **VAP Groups** - The VAP Group feature allows for grouping of multiple Virtual Access Points into one object to be provisioned to the wireless radio.
6. **Assign WEP Key (optional for WEP encryption)** - Up to 4 keys can be defined per-NSA wireless appliance, and WEP-enabled VAPs can use these 4 keys independently. WEP keys are configured on Wireless > Security page.
7. **Assign Virtual Access Points to Wireless Radio** - This feature allows you to choose which VAP group to assign to the radio. Only a single VAP Group can be assigned to a wireless radio, so ensure that all of the VAPs you wish to make available are assigned to this group.

## Network Zones

This section contains the following sub-sections:

- [“The Wireless Zone” section on page 355](#)
- [“Custom Wireless Zone Settings” section on page 355](#)

A network security zone is a logical method of grouping one or more interfaces with friendly, user-configurable names, and applying security rules as traffic passes from one zone to another zone. With the zone-based security, the administrator can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. Network Zones are configured from the **Network > Zones** page

Name	Security Type	Member Interfaces	Interface Trust	Content Filtering	Client AV	Gateway AV	Anti-Spyware	IPS	GSC	Configure
LAN	Trusted	X2	✓	✓		✓	✓	✓		⚙️
WAN	Untrusted	X1				✓	✓	✓		⚙️
DMZ	Public	N/A	✓	✓						⚙️
VPN	Encrypted	N/A								⚙️
MULTICAST	Untrusted	N/A								⚙️
WLAN	Wireless	X2								⚙️
VAP-Guest	Wireless	X2/V200								⚙️
VAP-Corporate	Wireless	X2/V50	✓	✓	✓	✓	✓	✓	✓	⚙️
VAP-Guest_Secure	Wireless	X2/V150	✓	✓	✓	✓	✓	✓	✓	⚙️
VAP-Legacy	Wireless	X2/V100	✓							⚙️
VAP-SSL-VPN	Wireless	X2/V250	✓	✓	✓	✓	✓	✓	✓	⚙️

For detailed information on configuring zones, see [“Network > Zones” section on page 191](#).

## The Wireless Zone

The Wireless Zone type, of which the “WLAN Zone” is the default instance, provides support to SonicWALL NSA wireless appliances. Each interface or sub-interface is assigned to a Wireless Zone, and that zone dictates security settings above the 802.11 layer, including WiFiSec Enforcement, SSL-VPN redirection, Wireless Guest Services, Lightweight Hotspot Messaging and all licensed Deep Packet Inspection security services.

## Custom Wireless Zone Settings

Although SonicWALL provides the pre-configured Wireless Zone, administrators also have the ability to create their own custom wireless zones. When using VAPs, a new wireless zone is created before each corresponding wireless sub-interface or Virtual Access Point. The following three sections describe settings for custom wireless zones:

- [“General” section on page 356](#)
- [“Wireless” section on page 357](#)
- [“Guest Services” section on page 358](#)

**General**

Feature	Description
Name	Create a name for your custom Zone
Security Type	Select <b>Wireless</b> in order to enable and access wireless security options.
Allow Interface Trust	Select this option to automatically create access rules to allow traffic to flow between the interfaces of a zone. This will effectively allow users on a wireless zone to communicate with each other. This option is often disabled when setting up Wireless Guest Services (WGS).
SonicWALL Security Services	Select the security services you wish to enforce on this zone. This allows you to extend your SonicWALL UTM security services to your SonicPoints.

## Wireless

**Wireless Settings**

Only allow traffic generated by a SonicPoint

SSL-VPN Enforcement

SSL-VPN server: --Select an address object--

SSL-VPN service: --Select a service--

WiFiSec Enforcement

WiFiSec Exception Service: --Select a service--

Require WiFiSec for Site-to-Site VPN Tunnel Traversal

Trust WPA/WPA2 traffic as WiFiSec

**SonicPoint Settings**

SonicPoint Provisioning Profile: SonicPoint

Feature	Description
Only allow traffic generated by a SonicPoint	Restricts traffic on this zone to SonicPoint-generated traffic only.
SSL-VPN Enforcement	Redirects all traffic entering the Wireless Zone to a defined SonicWALL SSL-VPN appliance. This allows all wireless traffic to be authenticated and encrypted by the SSL-VPN, using, for example, NetExtender to tunnel all traffic. Note: Wireless traffic that is tunneled through an SSL-VPN will appear to originate from the SSL-VPN rather than from the Wireless Zone. <b>SSL-VPN Server</b> - Select the Address Object representing the SSL-VPN appliance to which you wish to redirect wireless traffic.
WiFiSec Enforcement	Requires all traffic be either IPsec or WPA. With this option checked, all non-guest connections must be IPsec enforced. <b>WiFiSec Exception Service</b> - Select the service(s) you wish to be exempt from WiFiSec Enforcement.
Require WiFiSec for Site-to-site VPN Tunnel Traversal	For use with WiFiSec enforcement, requires WiFiSec security on all site-to-site VPN connections through this zone.
Trust WPA/WPA2 traffic as WiFiSec	Allows WPA or WPA2 to be used as an alternative to WiFiSec.
SonicPoint Provisioning Profile	Select a pre-defined SonicPoint Provisioning Profile to be applied to all current and future SonicPoints on this zone.

## Guest Services

The **Enable Wireless Guest Services** option allows the following guest services to be applied to a zone:

Feature	Description
Enable inter-guest communication	Allows guests connecting to SonicPoints in this Wireless Zone to communicate directly and wirelessly with each other.
Bypass AV Check for Guests	Allows guest traffic to bypass Anti-Virus protection
Enable Dynamic Address Translation (DAT)	Dynamic Address Translation (DAT) allows the zone to support any IP addressing scheme for WGS users.  If this option is disabled (un-checked), wireless guest users must either have DHCP enabled, or an IP addressing scheme compatible with the SonicPoint's network settings.
Enable External Guest Authentication	Requires guests connecting from the device or network you select to authenticate before gaining access. This feature, based on Lightweight Hotspot Messaging (LHM) is used for authenticating Hotspot users and providing them parametrically bound network access.
Custom Authentication Page	Redirects users to a custom authentication page when they first connect to the Wireless Zone. Click Configure to set up the custom authentication page. Enter either a URL to an authentication page or a custom challenge statement in the text field, and click OK.
Post Authentication Page	Directs users to the page you specify immediately after successful authentication. Enter a URL for the post-authentication page in the field.
Bypass Guest Authentication	Allows WGS to integrate into environments already using some form of user-level authentication. This feature automates the WGS authentication process, allowing wireless users to reach WGS resources without requiring authentication. This feature should only be used when unrestricted WGS access is desired, or when another upstream device is enforcing authentication.

Feature	Description
Redirect SMTP traffic to	Redirects SMTP traffic incoming on this zone to an SMTP server you specify. Select the address object to redirect traffic to.
Deny Networks	Blocks traffic from the networks you specify. Select the subnet, address group, or IP address to block traffic from.
Pass Networks	Automatically allows traffic through the Wireless Zone from the networks you select.
Max Guests	Specifies the maximum number of guest users allowed to connect to the Wireless Zone. The default is 10.

## WLAN Subnets

WLAN subnets are used to segment IP address space for use by Virtual Access Points (VAP). Each VAP must have a separate WLAN subnet, and you must create the WLAN subnet before creating the VAP. To create a WLAN subnet, complete the following steps.

**Step 1** Navigate to the **Network > Interfaces** page.

**Step 2** Click the **Add WLAN Subnet** button.

**Step 3** Configure the following options:

- **Zone:** By default, the zone is set to **WLAN**. You can select any other wireless zone that you have created on the **Network > Zones** page.

- **Subnet Name:** The name of the interface.
- **IP Address:** The first IP address in the subnet. Make sure that the IP address subnet does not conflict with another address range.
- **Subnet Mask:** 255.255.255.0 is the default
- **SonicPoint Limit:** The maximum number of allowed SonicPoints is configured automatically.
- **Comment:** Optionally enter a comment about the subnet.
- **Management:** Select the appropriate protocols to allow remote management of the SonicWALL security appliance from this subnet.
- **User Login:** Select HTTP and/or HTTPS to allow users with limited management rights to log in to the SonicWALL security appliance.
- **Add rule to enable redirect from HTTP to HTTPS:** If you select HTTPS but do not select HTTP for either Management or User Login, select this option to redirect HTTP users to HTTPS.
- **Create default DHCP Lease Scope:** Select to create a DHCP lease scope for this subnet. The DHCP lease scope consists of the IP addresses that are reserved for users who connect to the VAP associated with this WLAN subnet. This option is enabled by default.

To configure additional options for the DHCP lease scope (such as the number of IP addresses and the lease time), go to the **Network > DHCP Server** page, locate the lease scope in the DHCP Server Lease Scope table, and click on the **Configure** icon. See [“Network > DHCP Server” section on page 277](#) for more information.

**Step 4** Optionally, you can enable multicast reception on the subnet by clicking on the **Advanced** tab and selecting the **Enable multicast support** checkbox.

**Step 5** Click **OK**.

## DHCP Server Scope

The DHCP server assigns leased IP addresses to users within specified ranges, known as “Scopes”. The default ranges for DHCP scopes are often excessive for the needs of most SonicPoint deployments, for instance, a scope of 200 addresses for an interface that will only use 30. Because of this, DHCP ranges must be set carefully in order to ensure the available lease scope is not exhausted.

The DHCP scope should be resized as each interface/sub-interface is defined to ensure that adequate DHCP space remains for all subsequently defined interfaces. Failure to do so may cause the auto-creation of subsequent DHCP scopes to fail, requiring manual creation after performing the requisite scope resizing. DHCP Server Scope is set from the **Network > DHCP Server** page.

#	Type	Lease Scope	Interface	Details	Enable	Configure
<input type="checkbox"/> 1	Dynamic	Range: 10.10.10.2 - 10.10.10.246	X2		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 2	Dynamic	Range: 172.16.100.2 - 172.16.100.10	X2V100		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 3	Dynamic	Range: 172.16.150.2 - 172.16.150.25	X2V150		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 4	Dynamic	Range: 172.16.200.2 - 172.16.200.50	X2V200		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 5	Dynamic	Range: 172.16.250.2 - 172.16.250.50	X2V250		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 6	Dynamic	Range: 172.16.50.2 - 172.16.50.100	X2V50		<input checked="" type="checkbox"/>	
<input type="checkbox"/> 7	Dynamic	Range: 192.168.168.1 - 192.168.168.167	X0		<input checked="" type="checkbox"/>	



## Virtual Access Points Profiles

A Virtual Access Point Profile allows the administrator to pre-configure and save access point settings in a profile. VAP Profiles allows settings to be easily applied to new Virtual Access Points. Virtual Access Point Profiles are created by clicking the **Add...** button in the **Virtual Access Point Profiles** section of the **Wireless > Virtual Access Point** page.

#	Name	Type	Authentication	Cipher	Max Clients	Configure
<input type="checkbox"/> 1	Corporate-WPA2	SonicPoint	WPA2-EAP	TKIP	32	
<input type="checkbox"/> 2	Guest	SonicPoint	Open	None	32	
<input type="checkbox"/> 3	Guest_Secure-P	SonicPoint	WPA-PSK	TKIP	32	
<input type="checkbox"/> 4	Legacy-WEP	SonicPoint	Shared	WEP	32	

## Virtual Access Point Profile Settings

The table below lists configuration parameters and descriptions for Virtual Access Point Profile Settings:

Feature	Description
Radio Type	Set to <b>Wireless-Internal-Radio</b> by default. This is currently the only supported radio type.
Name	Choose a friendly name for this VAP Profile. Choose something descriptive and easy to remember as you will later apply this profile to new VAPs.
Authentication Type	<p>Below is a list available authentication types with descriptive features and uses for each:</p> <p>WPA</p> <ul style="list-style-type: none"> <li>• Good security (uses TKIP)</li> <li>• For use with trusted corporate wireless clients</li> <li>• Transparent authentication with Windows log-in</li> <li>• No client software needed in most cases</li> </ul> <p>WPA2</p> <ul style="list-style-type: none"> <li>• Best security (uses AES)</li> <li>• For use with trusted corporate wireless clients</li> <li>• Transparent authentication with Windows log-in</li> <li>• Client software install may be necessary in some cases</li> <li>• Supports 802.11i "Fast Roaming" feature</li> <li>• No backend authentication needed after first log-in (allows for faster roaming)</li> </ul> <p>WPA2-AUTO</p> <ul style="list-style-type: none"> <li>• Tries to connect using WPA2 security, if the client is not WPA2 capable, the connection will default to WPA.</li> </ul>
Unicast Cipher	The unicast cipher will be automatically chosen based on the authentication type.

Feature	Description
Multicast Cipher	The multicast cipher will be automatically chosen based on the authentication type.
Maximum Clients	Choose the maximum number of concurrent client connections permissible for this virtual access point.

### WPA-PSK / WPA2-PSK Encryption Settings

Pre-Shared Key (PSK) is available when using WPA or WPA2. This solution utilizes a shared key.

Feature	Description
Pass Phrase	The shared passphrase users will enter when connecting with PSK-based authentication.
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

### WPA-EAP / WPA2-EAP Encryption Settings

Extensible Authentication Protocol (EAP) is available when using WPA or WPA2. This solution utilizes an external 802.1x/EAP capable RADIUS server for key generation.

Feature	Description
Radius Server 1	The name/location of your Radius authentication server
Radius Server 1 Port	The port on which your Radius authentication server communicates with clients and network devices.
Radius Server 1 Secret	The secret passcode for your Radius authentication server
Radius Server 2	The name/location of your backup Radius authentication server
Radius Server 2 Port	The port on which your backup Radius authentication server communicates with clients and network devices.
Radius Server 2 Secret	The secret passcode for your backup Radius authentication server
Group Key Interval	The time period (in seconds) during which the WPA/WPA2 group key is enforced to be updated.

## Virtual Access Points

Virtual Access Points are configured from the **Wireless > Virtual Access Point** page by clicking the **Add...** button in the **Virtual Access Points** section.

#	SSID	VLAN ID	Authentication	Cipher	Max Clients	SSID Suppress	Enable	Configure
1	VAP-Guest	200	Open	None	32	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
2	VAP-LHM	350	Open	None	32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
3	VAP-Legacy	100	Shared	WEP	32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
4	VAP-Guest_Secu	150	WPA-PSK	TKIP	32	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
5	VAP-Corporate	50	WPA2-AUTO-EAP	TKIP	32	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

## General VAP Settings

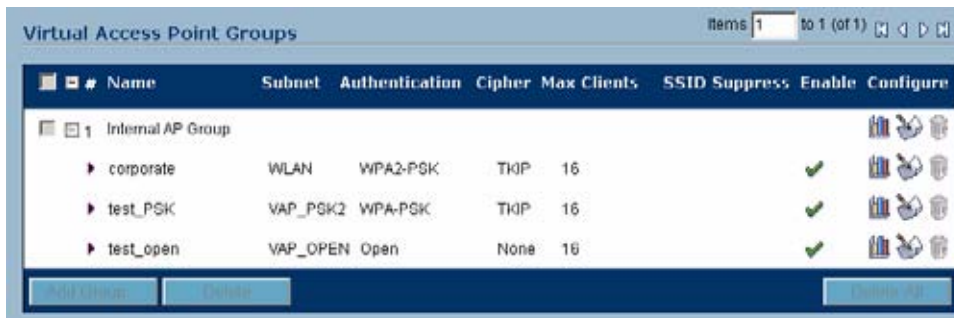
Feature	Description
SSID	Create a friendly name for your VAP.
Subnet name	Select the WLAN subnet that will be used for this VAP. The WLAN subnet must be created on the <b>Network &gt; Interfaces</b> page before you can create the VAP.
Enable Virtual Access Point	Enables this VAP.
Enable SSID Suppress	Suppresses broadcasting of the SSID name and disables responses to probe requests. Check this option if you do not wish for your SSID to be seen by unauthorized wireless clients.

## Advanced VAP Settings

Advanced settings allows the administrator to configure authentication and encryption settings for this connection. Choose a **Profile Name** to inherit these settings from a user created profile. See [“Virtual Access Points Profiles” section on page 361](#) for complete authentication and encryption configuration information.

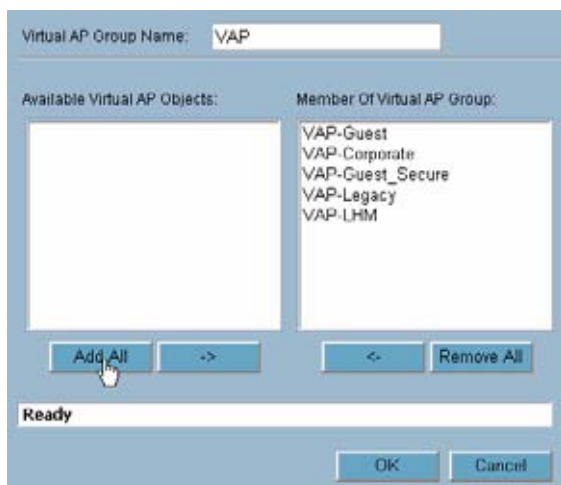
## Virtual Access Point Groups

The VAP Group feature allows for grouping of multiple VAP objects to be simultaneously applied to the integrated wireless radio of the SonicWALL security appliance. Virtual Access Point Groups are configured from the **Wireless > Virtual Access Point** page.



After you have created your VAPs, you must add them to the VAP group.

- Step 1** Click the **Configure** icon next to the Virtual Access Point group, which is named **Internal AP Group** by default. The **Edit Virtual Access Point Group** window displays.



- Step 2** Optionally, you can change the **Virtual AP Group Name**.
- Step 3** Select the desired VAPs from the list and click the **->** button to add them to the group. Optionally, click the **Add All** button to add all VAPs to a single group.
- Step 4** Press the **OK** button to save changes and create the group.

# Thinking Critically About VAPs

This section provides content to help determine what your VAP requirements are and how to apply these requirements to a useful VAP configuration. This section contains the following sub-sections:

- [“Determining Your VAP Needs” section on page 365](#)
- [“A Sample Network” section on page 365](#)
- [“Determining Security Configurations” section on page 366](#)
- [“VAP Configuration Worksheet” section on page 366](#)

## Determining Your VAP Needs

When deciding how to configure your VAPs, begin by considering your communication needs, particularly:

- How many different classes of wireless users do I need to support?
- How do I want to secure these different classes of wireless users?
  - Do my wireless client have the required hardware and drivers to support the chosen security settings?
- What network resources do my wireless users need to communicate with?
  - Do any of these wireless users need to communicate with other wireless users?
- What security services do I wish to apply to each of these classes or wireless users?

## A Sample Network

The following is a sample VAP network configuration, describing four separate VAPs:

- **VAP #1, Corporate Wireless Users** – A set of users who are commonly in the office, and to whom should be given full access to all network resources, providing that the connection is authenticated and secure. These users already belong to the network’s Directory Service, Microsoft Active Directory, which provides an EAP interface through IAS – Internet Authentication Services
- **VAP #2, Visiting Partners** – Business partners, clients, and affiliated who frequently visit the office, and who need access to a limited set of trusted network resources, as well as the Internet. These users are not located in the company’s Directory Services.
- **VAP #3, Guest Users** – Visiting clients to whom you wish to provide access only to untrusted (e.g. Internet) network resources. Some guest users will be provided a simple, temporary username and password for access.
- **VAP #4, Frequent Guest Users** – Same as Guest Users, however, these users will have more permanent guest accounts through a back-end database.

## Determining Security Configurations

Understanding these requirements, you can then define the Zones (and interfaces) and VAPs that will provide wireless services to these users:

- **Corp Wireless** – Highly trusted wireless Zone. Employs WPA2-AUTO-EAP security. WiFiSec (WPA) Enforced.
- **WEP & PSK** – Moderate trust wireless Zone. Comprises two virtual APs and sub-interfaces, one for legacy WEP devices (e.g. wireless printers, older handheld devices) and one for visiting clients who will use WPA-PSK security.
- **WGS** – Wireless Guest Services Zone, using the internal WGS user database.
- **LHM** – Lightweight Hotspot Messaging enabled Zone, configured to use external LHM authentication-back-end server.

## VAP Configuration Worksheet

The worksheet on the following page provides some common VAP setup questions and solutions along with a space for you to record your own configurations.

Questions	Examples	Solutions
How many different types of users will I need to support?	Corporate wireless, guest access, visiting partners, wireless devices are all common user types, each requiring their own VAP	Plan out the number of different VAPs needed. Configure a Zone and WLAN subnet for each VAP needed
	Your Configurations:	
How many users will each VAP need to support?	A corporate campus has 100 employees, all of whom have wireless capabilities	The DHCP scope for the visitor Zone is set to provide at least 100 addresses
	A corporate campus often has a few dozen wireless capable visitors	The DHCP scope for the visitor Zone is set to provide at least 25 addresses
	Your Configurations:	
How do I want to secure different wireless users?	A corporate user who has access to corporate LAN resources.	Configure WPA2-EAP
	A guest user who is restricted to only internet access	Enable WGS but configure no security settings
	A legacy wireless printer on the corporate LAN	Configure WEP and enable MAC address filtering
	Your Configurations:	
What network resources do my users need to communicate with?	A corporate user who needs access to the corporate LAN and all internal LAN resources, including other WLAN users.	Enable Interface Trust on your corporate zone.
	A wireless guest who needs to access internet and should not be allowed to communicate with other WLAN users.	Disable Interface Trust on your guest zone.
	Your Configurations:	

Questions	Examples	Solutions
What security services to I wish to apply to my users?	Corporate users who you want protected by the full SonicWALL security suite.	Enable all SonicWALL security services.
	Guest users who have no LAN access.	Disable all SonicWALL security services.
	Your Configurations:	



# **PART 5**

# **WWAN**





## CHAPTER 34

# Configuring Wireless WAN (TZ 190 only)

---

## WWAN

This chapter describes how to configure the Wireless WAN interface on the SonicWALL TZ 190 appliance. It contains the following sections:

- “Wireless WAN Overview” on page 371
- “Wireless WAN Prerequisites” on page 376
- “Viewing the WWAN Status” on page 377
- “Configuring Wireless WAN” on page 377
- “Monitoring WWAN Data Usage” on page 385
- “WWAN Glossary” on page 386

## Wireless WAN Overview

This section provides an overview of WWAN. It contains the following sections:

- “What is WWAN?” on page 371
- “Understanding Wireless WAN Connection Models” on page 372
- “Understanding WWAN Failover” on page 373
- “Wireless WAN PC Card Support” on page 376
- “3G Wireless WAN Service Provider Support” on page 376

## What is WWAN?

The SonicWALL TZ 190 security appliance introduces support for 3G (Third Generation) Wireless WAN connections that utilize data connections over 3G Cellular networks. The Wireless WAN (WWAN) can be used for:

- WAN Failover to a connection that is not dependent on wire or cable.
- Temporary networks where a pre-configured connection may not be available, such as trade-shows and kiosks.
- Mobile networks, where the SonicWALL TZ 190 is based in a vehicle.

- Primary WAN connection where wire-based connections are not available and 3G Cellular is.

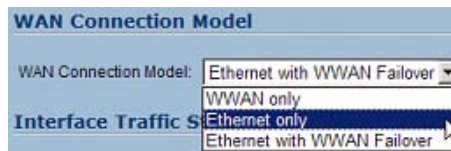
Wireless Wide Area Networks provide untethered remote network access through the use of mobile or cellular data networks. While legacy cellular networks, such as GSM, were only able to provide data rates of about 14 Kbps, today's emerging WWAN technologies (such as UMTS and HSDPA) provide theoretical data rates of up to 10 Mbps, rivaling many wired technologies.

The cellular networks powering Wireless Wide Area Networking have been evolving very quickly, and as a result comprise many different implementations. Fundamentally, they fall into two protocols:

- **GSM - Global System for Mobile Communication** - The most widely used protocol outside of the Americas. GSM is often regarded as less susceptible to signal degradation indoors. Although GSM is used both in the Americas and the rest of the world, the American implementation operates on a different frequency, and interoperability is not guaranteed unless explicitly supported by the equipment.
- **CDMA - Code Division Multiple Access** - The most widely used protocol in the Americas. CDMA has capacity advantages over GSM, but congestion tends to reduce its operating range.

## Understanding Wireless WAN Connection Models

The TZ190 provides flexible control over WAN connectivity with the **WAN Connection Model** setting. Accessible from the **Network > Interfaces** page of the management interface, the **WAN Connection Model settings** allows the administrator to precisely control the behavior of the WWAN connection. The three settings are as follows:



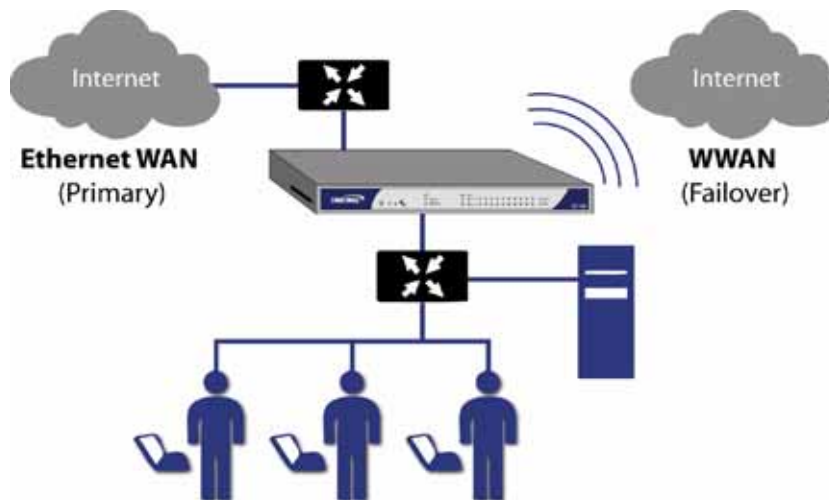
- **WWAN Only** – For use when the WWAN is the only WAN connection in use on the TZ190.
- **Ethernet Only** – For use when the WWAN is to be disabled. The Ethernet WAN (the WAN port, OPT port, or both) is the only WAN connection in use on the TZ190.
- **Ethernet with WWAN Failover** – For use when both the WWAN and the Ethernet WAN (the WAN port, OPT port, or both) are to serve as WAN connections on the TZ190.

In addition to the WAN Connection Model setting, the following changes were also introduced in SonicOS Enhanced 3.6 (and later versions) to optimize the operation of the WWAN interface:

- To more accurately reflect the operation of WAN load balancing and Failover sub-system, the **WAN Failover & LB** page has been renamed to **Ethernet LB**.
- Failover between the Ethernet WAN (the WAN port, OPT port, or both) and the WWAN is supported through the **WAN Connection Model** setting, but Load-balancing is currently only supported on Ethernet WAN interfaces. WWAN interface traffic statistics will continue to be displayed in the WAN Load Balancing Statistics table on the **Network > Ethernet LB** page.
- The WAN Load-balancing and Failover sub-system is now permanently enabled for more transparent support of the **WAN Connection Model** setting. This was previously controlled by the **Enable Load Balancing** setting on the **WAN Failover & LB** page.
- WWAN interface probe monitoring appears on the **WWAN > Settings** page under the **WWAN Probe Settings** heading. (Ethernet WAN interface probe settings is unchanged on the **Network > Ethernet LB** page under the **WAN Interfaces Monitoring** section.)

## Understanding WWAN Failover

When the **WAN Connection Model** is set to **Ethernet with WWAN Failover**, the WAN (Ethernet) interface is the primary connection. If the WAN interface fails, the SonicWALL TZ 190 fails over to the WWAN interface.



**Note**

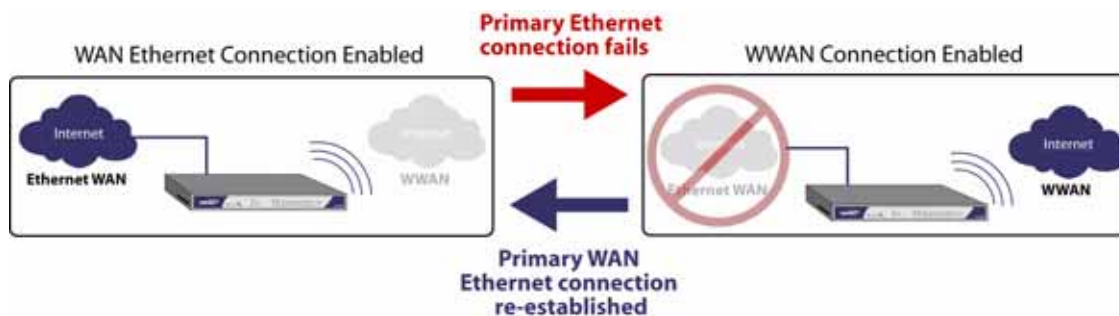
It is important to note that the WAN-to-WWAN failover process is different for the three different WWAN Connection Profile dial types: **Persistent**, **Dial on Data**, and **Manual Dial**.

The following sections describe the three different methods of WAN-to-WWAN failover:

- “Persistent Connection WWAN Failover” on page 373
- “Dial on Data WWAN Failover” on page 374
- “Manual Dial WWAN Failover” on page 375

### Persistent Connection WWAN Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the WWAN Connection Profile is configured for **Persistent Connection**.



1. **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. WWAN is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies WWAN as the destination interface).
2. **Primary Ethernet connection fails** – The WWAN connection is initiated and remains in an “always-on” state while the Ethernet WAN connection is down.

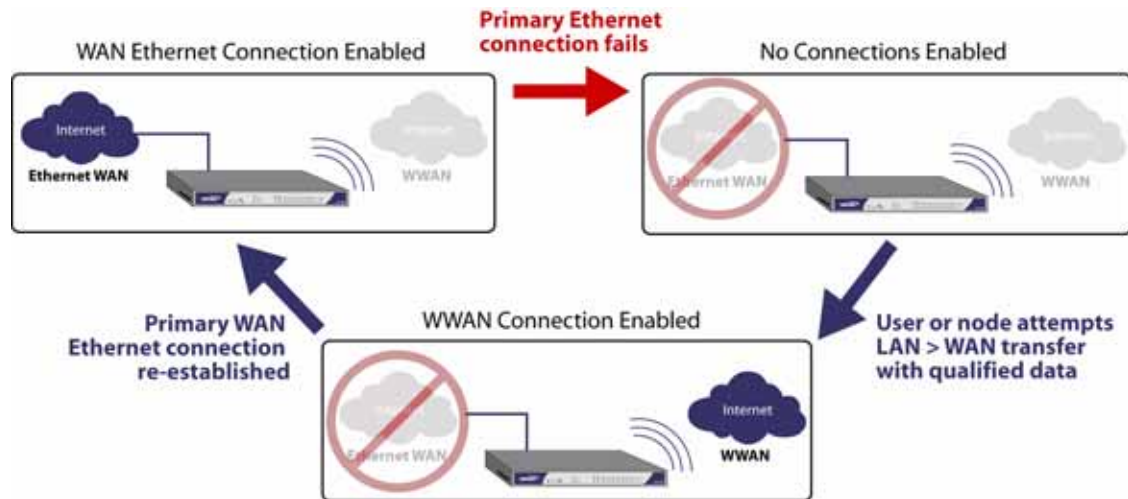
If a secondary Ethernet WAN (the OPT port) is configured, the TZ190 will first failover to the secondary Ethernet WAN before failing over to the WWAN. In this situation, WWAN failover will only occur when both the WAN and OPT paths are unavailable.

3. **Reestablishing Primary Ethernet Connectivity After Failover** – When the Ethernet WAN connection (either the WAN port or the OPT port, if so configured) becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. This includes active connections and VPN connections. The WWAN connection is closed.

**Caution** It is not recommended to configure a policy-based route that uses the WWAN connection when the **WAN Connection Model** is set for **Ethernet with WWAN Failover**. If a policy-based route is configured to use the WWAN connection, the connection will remain up until the Maximum Connection Time (if configured) is reached.

### Dial on Data WWAN Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the WWAN Connection Profile is configured for **Dial on Data**.



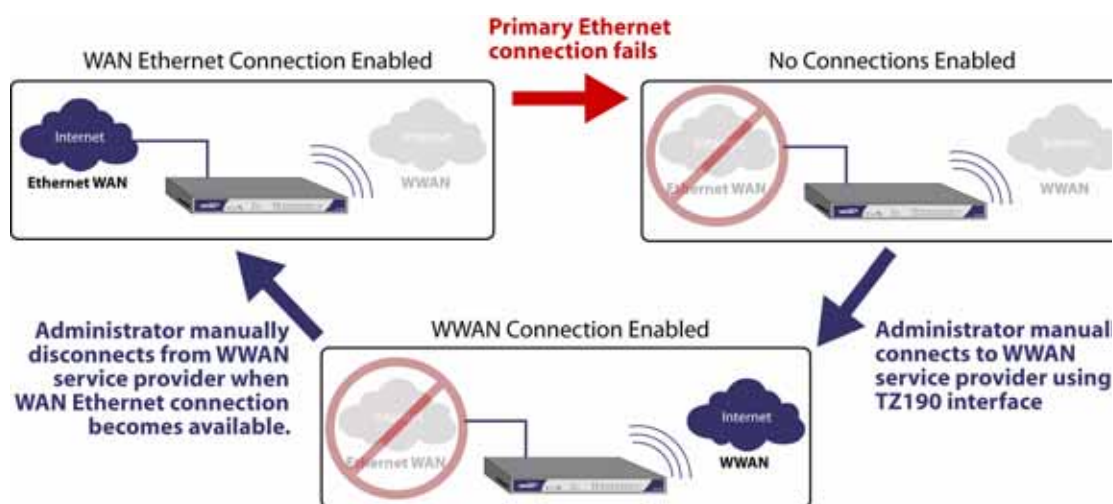
1. **Primary Ethernet connection available** – The Ethernet WAN interface is connected and used as the primary connection. WWAN is never connected while the Ethernet WAN interface is available (unless an explicit route has been configured which specifies WWAN as the destination interface).
2. **Primary Ethernet Connection Fails** – The WWAN connection is not established until qualifying outbound data attempts to pass through the SonicWALL TZ 190 appliance.
3. **WWAN Connection Established** – The WWAN connection is established when the device or a network node attempts to transfer qualifying data to the Internet. The WWAN connection stays enabled until the *Maximum Connection Time (if configured)* is reached.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – When an Ethernet WAN connection becomes available again, all LAN-to-WAN traffic is automatically routed back to the available Ethernet WAN connection. The WWAN connection is closed.

**Caution** It is not recommended to configure a policy-based route that uses the WWAN connection when the **WAN Connection Model** is set for **Ethernet with WWAN Failover**. If a policy-based route is configured to use the WWAN connection, the connection will remain up until the Maximum Connection Time (if configured) is reached.

### Manual Dial WWAN Failover

The following diagram depicts the sequence of events that occur when the WAN ethernet connection fails and the WWAN Connection Profile is configured for **Manual Dial**.

**Caution** It is not recommended to use a **Manual Dial** WWAN Connection Profile when the **WAN Connection Model** is set for **Ethernet with WWAN Failover**. The **Manual Dial** WWAN Connection Profile is only intended to be used when the device's WAN Connection Model is set to **WWAN Only** in the **Network > Interfaces** page.



1. **Primary Ethernet Connection Available** - The Ethernet WAN is connected and used as the primary connection. WWAN is never connected while the Ethernet WAN connection is available.
2. **Primary Ethernet Connection Fails** - The WWAN connection is not established until the administrator manually enables the connection.
3. **WWAN Connection Established** – A WWAN connection is established when the administrator manually enables the connection on the SonicWALL TZ 190. The WWAN connection stays enabled until the administrator manually disables the connection.
4. **Reestablishing WAN Ethernet Connectivity After Failover** – Regardless of whether the an Ethernet connection becomes available again, **all LAN-to-WAN traffic will still use the manually enabled WWAN connection** until the connection is manually disabled by the administrator. After a manual disconnect, the available Ethernet connection will be used.

## Wireless WAN PC Card Support

To use the wireless WAN interface you must have a wireless WAN PC card and a contract with a wireless service provider. Because both GSM and CDMA provide virtually the same performance, a WWAN service provider should be selected based primarily on the availability of supported hardware. SonicOS Enhanced 3.6 (and later versions) and the SonicWALL TZ 190 support the following wireless WAN PC cards (this list subject to change):

- Option Globe Trotter GTmax World (GPRS/EDGE/UMTS/HSDPA)
- Option Globe Trotter HSDPA (GPRS/EDGE/UMTS/HSDPA)
- Sierra Wireless Aircard 860 (GPRS/EDGE/UMTS/HSDPA)
- Sprint Novatel Merlin S620 (CDMA/EVDO)
- Sprint Novatel Merlin S720 (CDMA/EVDO)
- Verizon Wireless V620 (CDMA/EVDO)

## 3G Wireless WAN Service Provider Support

SonicOS Enhanced 3.6 (and later versions) and the SonicWALL TZ 190 support the following 3G Wireless network providers (this list is subject to change):

- Cingular Wireless
- H3G
- Sprint PCS Wireless
- Verizon Wireless
- Vodafone
- Telecom Italia Mobile
- Telefonica
- T-Mobile
- TDC Song
- Orange

## Wireless WAN Prerequisites

Before configuring the Wireless WAN interface on the SonicWALL TZ 190, you must complete the following prerequisites:

- Purchase a wireless WAN service plan from a supported third-party wireless provider
- Configure and activate your wireless WAN PC card
- Insert the Wireless WAN PC card into the SonicWALL TZ 190

For information on configuring these prerequisites, see the *SonicWALL TZ 190 Getting Started Guide*.



## Viewing the WWAN Status

The **WWAN > Status** page displays the current status of WWAN on the SonicWALL TZ190. It indicates the status of the WWAN connection, the current active WAN interface, or the current backup WAN interface. It also displays IP address information, DNS server addresses, the current active dial up profile, and the current signal strength.

The screenshot shows the SonicWALL management interface with the **WWAN > Status** page selected. The left sidebar contains navigation options: System, Network, WWAN, Status, Settings, Advanced, Connection Profiles, Data Usage, SonicPoint, Firewall, VoIP, VPN, Users, Security Services, Log, Wizards, Help, and Logout. The main content area displays the following information:

WWAN Status	
The modem is currently the active WAN interface	
WAN Gateway (Router)Address:	166.214.201.74
WAN IP (NAT Public) Address:	168.214.201.74
WAN Subnet Mask:	255.255.255.0
DNS Server 1:	10.11.12.13
DNS Server 2:	10.11.12.14
DNS Server 3:	0.0.0.0
Current Active Dial-up Profile (id):	Cingular (Standard) (1)

Signal Strength: Excellent (-51 dBm)

status: Ready

## Configuring Wireless WAN

To configure the Wireless WAN interface on the SonicWALL TZ 190 appliance, complete the following tasks:

- “Configuring WWAN Basic Settings” on page 377
- “Configuring WWAN Advanced Settings” on page 380
- “Configuring WWAN Connection Profiles” on page 381
- “Configuring the Maximum Allowed WWAN Connections” on page 384
- “Managing WWAN Connections” on page 384
- “Specifying the WAN Connection Model” on page 385

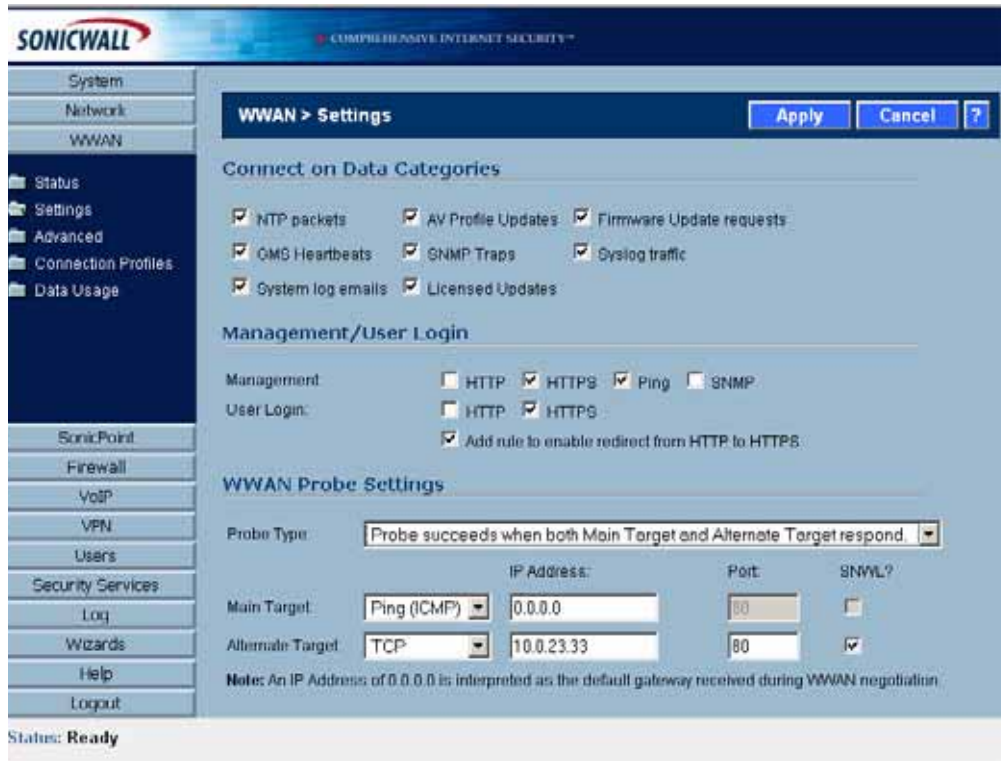
Most of the WWAN settings can also be configured on the **Network > Interfaces** page. WWAN Connection Profiles can only be configured on the **WWAN > Connection Profiles** page. The maximum number of hosts allowed to connect to the WWAN interface can only be configured on the **Network > Interfaces** page. See “Configuring the Wireless WAN Interface” on page 152 for more information.

## Configuring WWAN Basic Settings

On the **WWAN > Settings** page, you can configure the following three settings:

- “Connect on Data” on page 378

- “Management/User Login” on page 379
- “WWAN Probe Settings” on page 379



**Connect on Data**

The **Connect on Data Categories** settings allow you to configure the WWAN interface to automatically connect to the WWAN service provider when the SonicWALL TZ 190 detects specific types of traffic.

The **Connect on Data Categories** include:

- NTP packets
- GMS Heartbeats
- System log e-mails
- AV Profile Updates
- SNMP Traps
- Licensed Updates
- Firmware Update requests
- Syslog traffic

To configure the SonicWALL TZ 190 for Connect on Data operation, you must select **Dial on Data** as the **Dial Type** for the Connection Profile. See “**Configuring WWAN Connection Profiles**” on page 381 for more details.

## Management/User Login

The **Management/User Login** section must be configured to enable remote management of the SonicWALL TZ 190 appliance over the WWAN interface.



You can select any of the supported management protocol(s): **HTTPS**, **Ping**, and/or **SNMP**. You can also select **HTTP** for management traffic. However, bear in mind that HTTP traffic is less secure than HTTPS.

Select **Add rule to enable redirect from HTTP to HTTPS** to have the SonicWALL automatically convert HTTP requests to HTTPS requests for added security. This option is only available

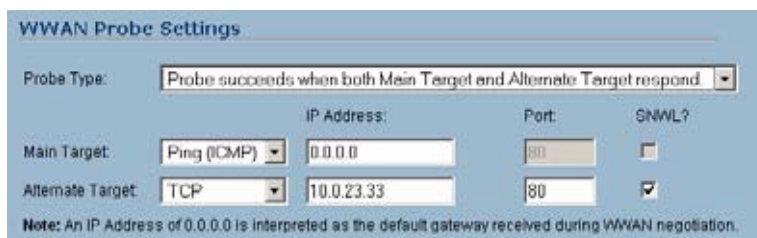
## WWAN Probe Settings

The **WWAN Probe Settings** section enables administrators to configure the WWAN interface to monitor the connection to the service provider and automatically disable the WWAN interface if the WWAN connection fails.



**Note**

If the Probe Target is unable to contact the target device, the WWAN interface is deactivated and traffic is no longer sent to the WWAN.



5. In the **WWAN Probe Settings** menu, select one of the following options:
  - ◆ **Probe succeeds when either Main Target or Alternate Target responds**
  - ◆ **Probe succeeds when both Main Target and Alternative Target respond**
  - ◆ **Probe succeeds when Main Target responds**
  - ◆ **Succeeds Always (no probing)**
6. For both the **Main Target** and, when applicable, the **Alternate Target** configure the following:
  - a Select **Ping (ICMP)** or **TCP** from the **Probe Target** menu.
  - b Enter the IP address of the main target device in the **IP Address** field.



**Tip**

To have the SonicWALL security appliance send WWAN probes to the default gateway received during WWAN negotiation, leave the IP address field as **0.0.0.0**.

- c If the probe target is using TCP, enter a port number in the **Port** field.
- d Check the **SNWL?** box if the target device is a SonicWALL security appliance. Do not check the **SNWL?** box for third-party devices, as the TCP probes may not work consistently.

## Configuring WWAN Advanced Settings

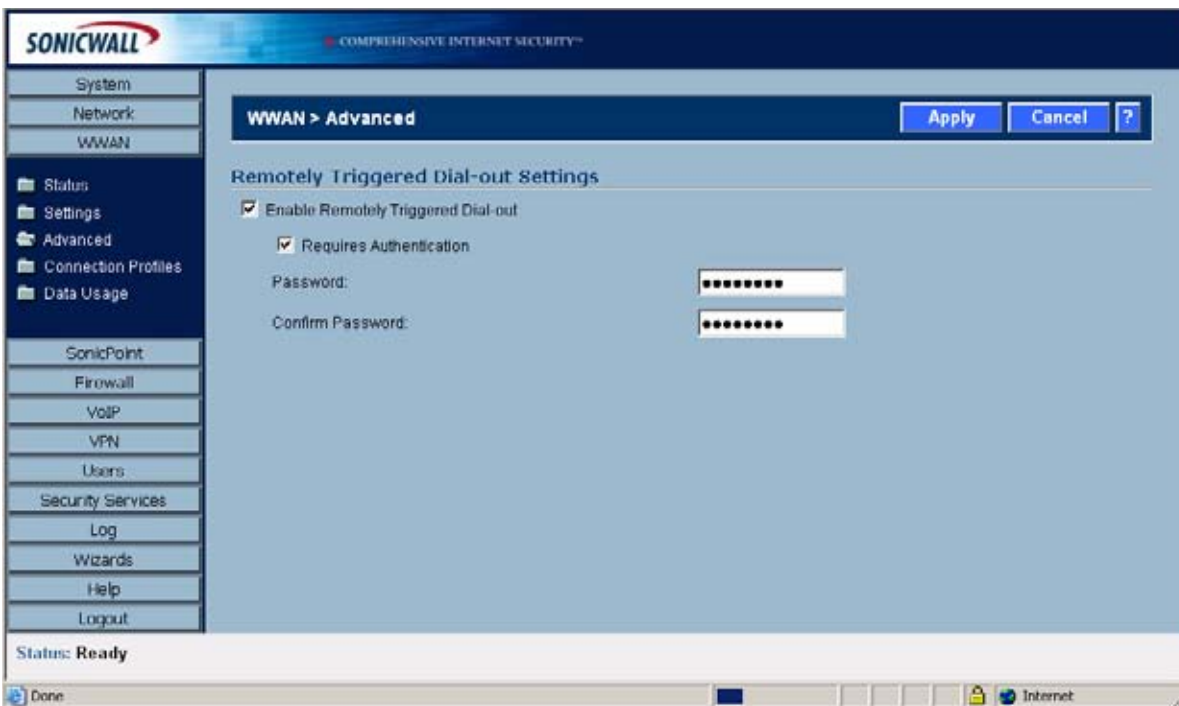
The **WWAN > Advanced** page is used to configure the Remotely Triggered Dial-Out feature on the SonicWALL TZ 190. The Remotely Triggered Dial-Out feature enables network administrators to remotely initiate a WWAN connection from a SonicWALL TZ 190.

### Configuring Remotely Triggered Dial-Out

Before configuring the Remotely Triggered Dial-Out feature, ensure that your configuration meets the following prerequisites:

- The WWAN profile is configured for **dial-on-data**.
- The SonicWALL Security Appliance is configured to be managed using **HTTPS**, so that the device can be accessed remotely.
- It is recommended that you enter a value in the **Enable Max Connection Time (minutes)** field. This field is located in the **WWAN Profile Configuration** window on the **Parameters** tab. See “Configuring WWAN Connection Profiles” on page 381 for more information. If you do not enter a value in this field, dial-out calls will remain connected indefinitely, and you will have to manually terminate sessions by clicking the **Disconnect** button.

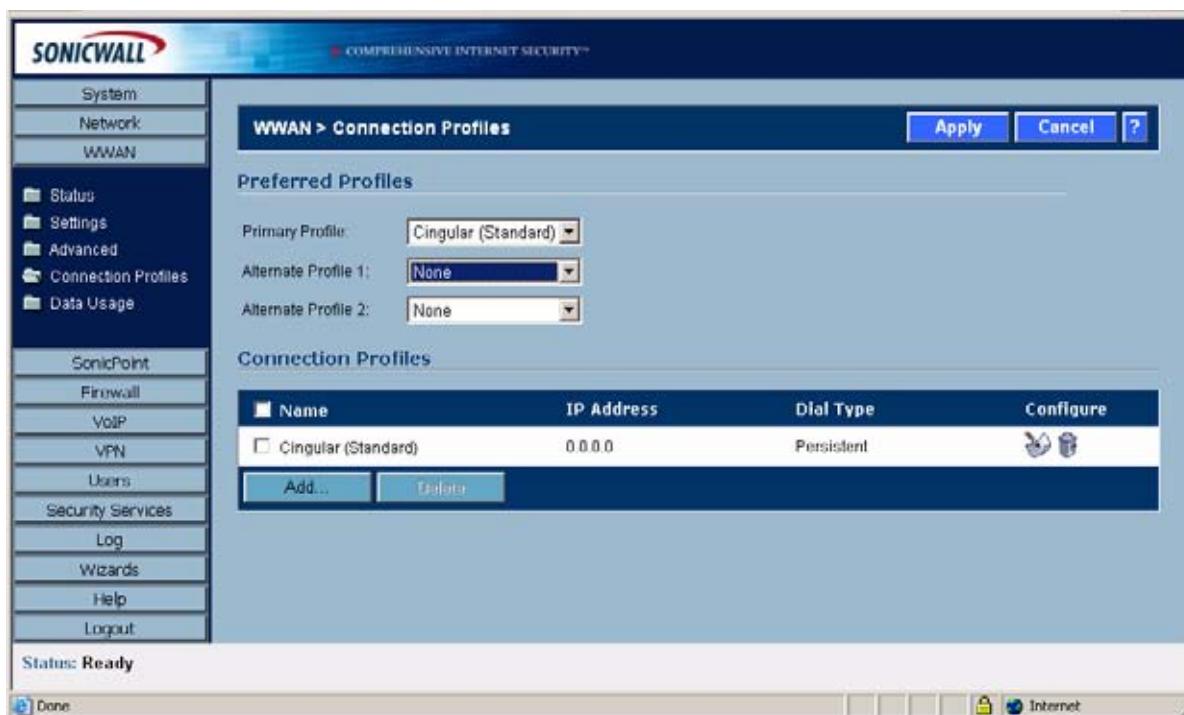
To configure Remotely Triggered Dial-Out, go the **WWAN > Advanced** screen.



7. Check the **Enable Remotely Triggered Dial-Out** checkbox.
8. (Optional) To authenticate the remote call, check the **Requires authentication** checkbox and enter the password in the **Password:** and **Confirm Password:** fields.

## Configuring WWAN Connection Profiles

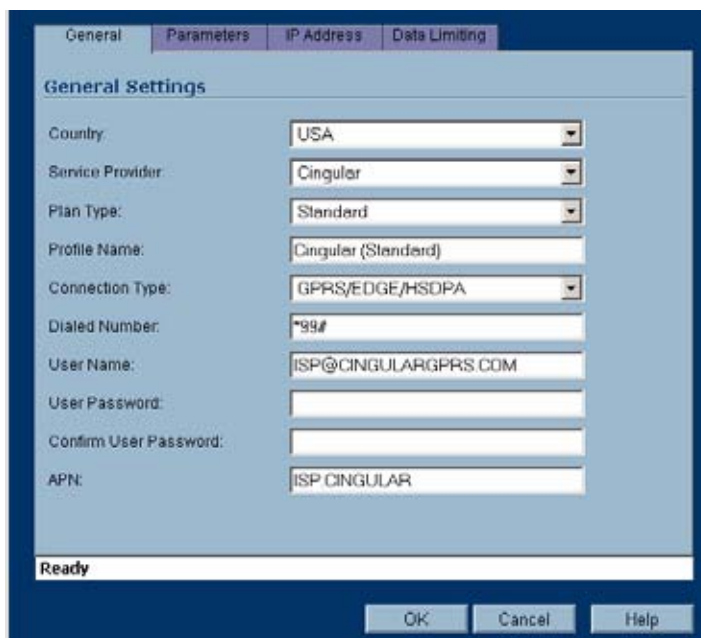
Use the **WWAN > Connection Profiles** to configure WWAN connection profiles and set the primary and alternate profiles.



Select the Primary WWAN connection profile in the **Primary Profile** pulldown menu. Optionally, you can select up to two alternate WWAN profiles.

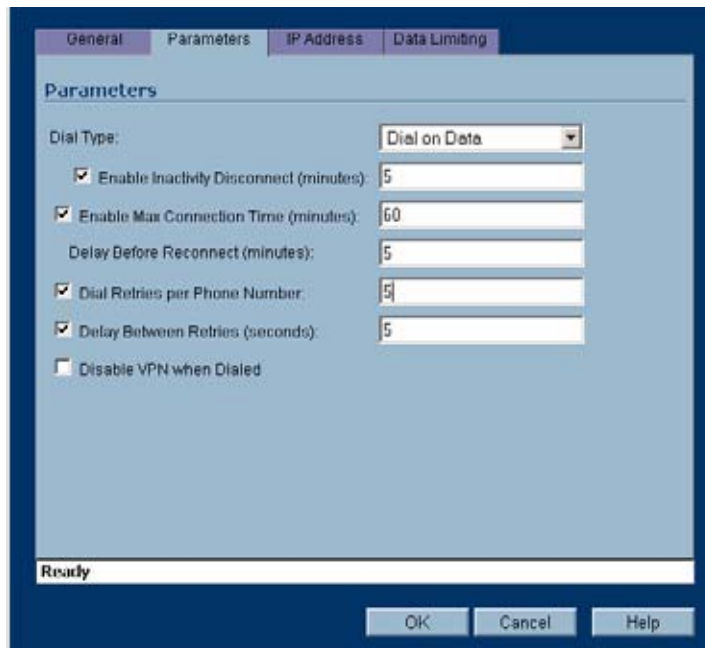
To create a WWAN connection profile, perform the following steps:

1. On the **WWAN > Connection Profiles** page, click on the **Add** button. The **WWAN Profile Configuration** window displays.



2. Select the **Country** where the SonicWALL TZ 190 appliance is deployed.

3. Select the **Service Provider** that you have created an account with. Note that only service providers supported in the country you selected are displayed.
4. In the **Plan Type** window, select the WWAN plan you have subscribed to with the service provider. If your specific plan type is listed in the pulldown menu, the rest of the fields in the **General** tab are automatically provisioned. Verify that these fields are correct and click on the **Parameters** tab.
5. If your **Plan Type** is not listed in the pulldown menu, select **Other**.
6. Enter a name for the WWAN profile in the **Profile Name** field.
7. Verify that the appropriate **Connection Type** is selected. Note that this field is automatically provisioned for most service providers.
8. Verify that the **Dialed Number** is correct. Note that the dialed number is **\*99#** for most Service Providers.
9. Enter your username and password in the **User Name**, **User Password**, and **Confirm User Password** fields, respectively.
10. Enter the Access Point Name in the **APN** field. APNs are required only by GPRS devices and will be provided by the service provider.
11. Click on the **Parameters** tab.



12. In the **Dial Type** pulldown menu, select whether the connection profile is a **Persistent Connection**, **Dial on Data**, or **Manual Dial**.

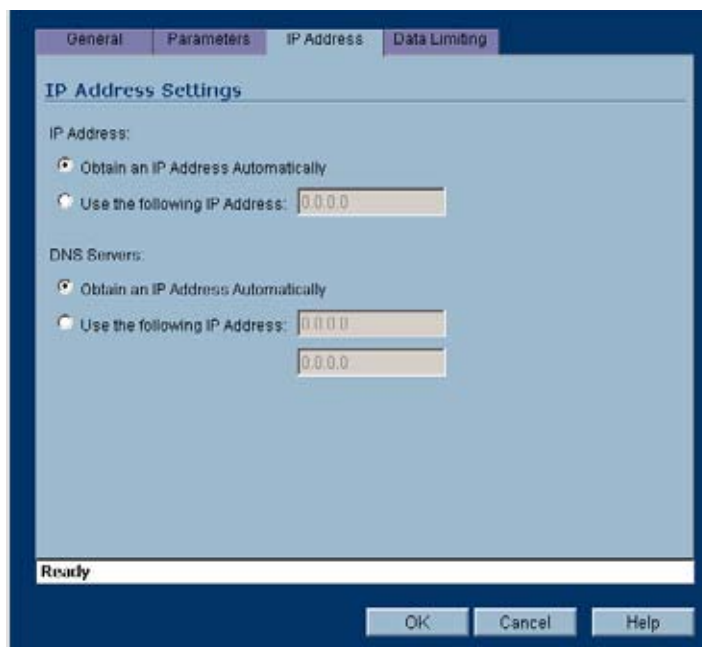
For a detailed explanation of how the different **Dial Types** operate when the **WAN Connection Types** is set for **Ethernet with WWAN Failover** see “Understanding WWAN Failover” on page 373.



**Note**

To configure the SonicWALL TZ 190 for remotely triggered dial-out, the **Dial Type** must be **Dial on Data**. See “**Configuring WWAN Advanced Settings**” on page 380 for more information.

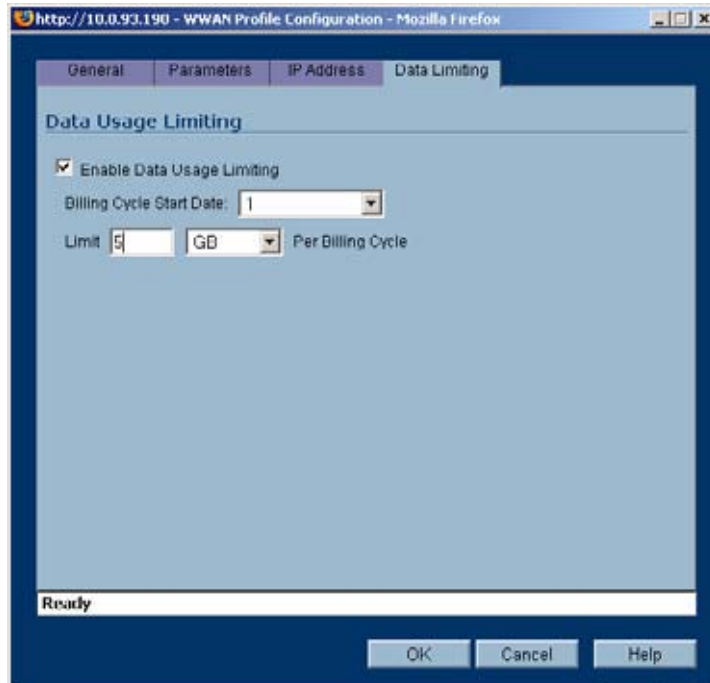
13. Select the **Enable Inactivity Disconnect (minutes)** checkbox and enter a number in the field to have the WWAN connection disconnected after the specified number of minutes of inactivity. Note that this option is not available if the **Dial Type** is **Persistent Connection**.
14. Select the **Enable Max Connection Time (minutes)** checkbox and enter a number in the field to have the WWAN connection disconnected after the specified number of minutes, regardless if the session is inactive or not. Enter a value in the **Delay Before Reconnect (minutes)** to have the SonicWALL TZ 190 automatically reconnect after the specified number of minutes.
15. Select the **Dial Retries per Phone Number** checkbox and enter a number in the field to specify the number of times the SonicWALL TZ 190 is to attempt to reconnect.
16. Select the **Delay Between Retries (seconds)** checkbox and enter a number in the field to specify the number of seconds between retry attempts.
17. Select the **Disable VPN when Dialed** checkbox to disable VPN connections over the WWAN interface.
18. Click on the **IP Addresses** tab.



By default, WWAN connection profiles are configured to obtain IP addresses and DNS server addresses automatically. To specify a static IP address, select the **Use the following IP Address** radio box and enter the IP address in the field.

To manually enter DNS server addresses, select the **Use the following IP Address** radio box and enter the IP addresses of the primary and secondary DNS servers in the fields.

19. Click on the **Data Limiting** tab.



Tip

If your WWAN account has a monthly data or time limit, it is strongly recommended that you enable Data Usage Limiting.

20. Select the **Enable Data Usage Limiting** checkbox to have the WWAN interface become automatically disabled when the specified data or time limit has been reached for the month.
21. Select the day of the month to start tracking the monthly data or time usage in the **Billing Cycle Start Date** pulldown menu.
22. Enter a value in the **Limit** field and select the appropriate limiting factor: either **GB**, **MB**, **KB**, or **minutes**.
23. Click **OK**.

## Configuring the Maximum Allowed WWAN Connections

To configure the maximum number of nodes allowed to connect to the WWAN interface, navigate to the **Network > Interfaces** page, click on the **Configure** icon for the **WWAN** interface. The **WWAN Settings** window is displayed. Click on the **Advanced** tab and enter the maximum number of nodes in the **Max Host** field. Entering **0** in the **Max Host** fields allows any number of nodes to connect.

See “Configuring the Wireless WAN Interface” on page 152 for more information.

## Managing WWAN Connections

To initiate a WWAN connection, perform the following steps, click on the **Manage** button in the **WWAN** interface line on the **Network > Interfaces** page. The **WWAN Connection** window displays. Click the **Connect** button. The SonicWALL TZ 190 attempts to connect to the WWAN service provider.



To disconnect a WWAN connection, click on the **Manage** button. The **WWAN Connection** window displays. Click **Disconnect**.

See “Configuring the Wireless WAN Interface” on page 152 for more information.

## Specifying the WAN Connection Model

To configure the WAN connection model, navigate to the **Network > Interfaces** page and select one of the following options in the **WAN Connection Model** pulldown menu:

- **WWAN only** - The WAN interface is disabled and the WWAN interface is used exclusively.
- **Ethernet only** - The WWAN interface is disabled and the WAN interface is used exclusively.
- **Ethernet with WWAN Failover** - The WAN interface is used as the primary interface and the WWAN interface is disabled. If the WAN connection fails, the WWAN interface is enabled and a WWAN connection is automatically initiated.

See “Configuring the Wireless WAN Interface” on page 152 for more information.

## Monitoring WWAN Data Usage

On the **WWAN > Data Usage** page, you can monitor the amount of data transferred over the WWAN interface in the **Data Usage** table and view details of WWAN sessions in the **Session History** table.

The screenshot shows the SonicWall management interface. The left sidebar contains navigation options: System, Network, WWAN, Status, Settings, Advanced, Connection Profiles, Data Usage, SonicPoint, Firewall, VoIP, VPN, Users, Security Services, Log, Wizards, Help, and Logout. The main content area is titled "WWAN > Data Usage" and includes a "Refresh" button. Below the title is a "Data Usage" section for "Cingular (Standard)" with a table showing usage for Year, Month, Week, Day, and Billing Cycle (10/1 - 10/31). Each row has a "Reset" button. Below this is a "Session History" table with columns for Session, Profile, Start Time, Duration, Total, Tx, Rx, and Properties. A tooltip is visible over the Properties column for session 2, showing details like Provider, Plan, User, Phone, IP, and DNS. A status message at the bottom reads "Status: The configuration has been updated."

Category	Usage	Action
Year:	20.38 KB, 2204 Minutes	Reset
Month:	20.38 KB, 2204 Minutes	Reset
Week:	1.65 KB, 971 Minutes	Reset
Day:	538 Bytes, 575 Minutes	Reset
Billing Cycle (10/1 - 10/31):	0.0 Bytes, 0 Minutes	Reset

Session	Profile	Start Time	Duration	Total	Tx	Rx	Properties
1	Cingular (Standard)	10/19/2006 08:32:07.720	07:50:12	28 Bytes	17 Bytes	11 Bytes	Properties
2	Cingular (Standard)	10/18/2006 17:23:25.240	08:21:10	1.6 KB	0 Bytes	0 Bytes	Properties
3	Cingular (Standard)	10/11/2006 13:44:12.000	Unknown	11 Bytes	0 Bytes	0 Bytes	Properties
4	Cingular (Standard)	10/11/2006 11:44:04.000	Unknown	0.0 Bytes	0 Bytes	0 Bytes	Properties
5	Cingular (Standard)	09/27/2006 10:30:40.000	Unknown	151.73 KB	109.74 KB	42.00 KB	Properties
6	Cingular (Standard)	09/28/2006 04:53:16.000	Unknown	249 Bytes	137 Bytes	112 Bytes	Properties

The **Data Usage** table displays the current data usage and online time for the current **Year**, **Month**, **Week**, **Day**, and **Billing Cycle**. Billing cycle usage is only calculated if the **Enable Data Usage Limiting** option is enabled on the WWAN Connection Profile.

Click the appropriate **Reset** button to reset any of the data usage categories.

**Note**

The **Data Usage** table is only estimate of the current usage and should not be used to calculate actual charges. Contact your Service Provider for accurate billing information.

The **Session History** table displays a summary of information about WWAN sessions. To view additional details about a specific session, place your mouse cursor over the **Properties** balloon.

## WWAN Glossary

- **1xRTT - Single Carrier Radio Transmission Technology** - The second generation of the CDMA protocol, permitting many radios to simultaneously share the same frequency. 1xRTT was mostly deployed in the Americas, but is now undergoing an evolution to 1xEV-DO by many operators.
- **1xEV-DO - Single Carrier Evolution Data Optimized (Also EV-DO)** - The evolution of the 1xRTT protocol, EV-DO provides true 3G speeds, competing with UMTS, but remains most widely used in the Americas. There are currently two revisions of EV-DO available: Rev. 0, which provides data rates up to 2.4 Mbps, and Rev. A, with data rates up to 3.1 Mbps.
- **APN - Access Point Name** - Designated the external connection point (access point) for devices on a GPRS network. APN designation is only required by GPRS devices, and will be provided by the network operator. APN uses a notation such as "general.t-mobile.uk", "btmobile.bt.com" and "wap.cingular".
- **DMA - Code Division Multiple Access** - A multiplexing technique that allows for multiple concurrent accesses to a channel through the use of unique data encoding rather than time or frequency based division of access. CDMA has capacity advantages over GSM, but congestion tends to reduce its operating range. Also refers to Qualcomm's family of protocols.
- **EDGE - Enhanced Data rates for GSM Evolution** - Also known as Enhanced GPRS. EDGE is an adaptive GPRS implementation employed by many GSM networks. It improves upon GPRS by using up to 8 time-slots (as opposed to a maximum of 5) with a denser modulation scheme for higher data rates. EDGE is regarded as a cost-saving interim GSM protocol until more widespread adoption of UMTS is seen, and it is currently broadly available in all worldwide geographies.
- **ESN - Electronic Serial Number** - A 32 bit number used to uniquely identify stations on a CDMA network. ESNs are the effective equivalent of GSM's IMEI scheme.
- **Generation** - WWAN protocols are divided by generation, such as 2G, 2.5G, and 3G, where 1G would be the original analog cellular networks. Generations advanced is usually characterized by improvements in speed and capacity. Although 3G is most commonly used to describe Wireless Wide Area Networking, 3G only refers to a single set of available protocols. A list of popular protocols by generation:
  - ◆ **1G** - Analog
  - ◆ **2G** - GSM
  - ◆ **2.5G** - GPRS
  - ◆ **2.75G** - EDGE, 1xRTT
  - ◆ **3G** - UMTS, 1xEV-DO
  - ◆ **3.5G** - HSDPA
- **GPRS - General Packet Radio Service** - An evolution of the GSM network that achieves speed improvements through the use of unused TDMA channels. GPRS is divided by incrementing classes, which define the number of time-slots and the data-rate per time-slot.

GPRS has an additional advantage over GSM in that it is a packet-switched technology, meaning that stations only send data when there is data to send (rather than reserving the entire channel as occurs in GSM's circuit-switched networks) thus making more efficient use of available bandwidth. The process of connecting to a GPRS network generally involves attachment to the network, followed by the construction and activation of a PDP context, as performed by a series of AT commands. This process is largely automated by SonicOS through the use of profiles, but also allows for manual PDP context construction.

- **GSM - Global System for Mobile Communication** - TDMA based protocol that uses digital channels for both signaling and speech, making it a well suited platform for data communications, although at very low data rates. GSM competes as a protocol with Qualcomm's CDMA, but remains the most popular worldwide protocol. GSM implementations are often regarded as less susceptible to signal degradation indoors. Although GSM is used both in the Americas and the rest of the world, the American implementation operates on a different frequency, and interoperability is not guaranteed unless explicitly supported by the equipment.
- **HSDPA - High Speed Downlink Packet Access** - An evolution of UMTS (and thus of GSM) based on W-CDMA technology. HSDPA can achieve very high data rates, with subsequent phases targeting rates of up to 50 Mbps, but it is not currently very widely adopted despite announcements of future support from many operators.
- **IMEI - International Mobile Equipment Identity** - A unique 15 digit number assigned to every GSM/UMTS device for the purposes of identifying the device (not the subscriber) on the network. The subscriber on these networks is identified by the IMSI number, which is stored on the SIM card.
- **IMSI - International Mobile Subscriber Identity** - A unique 15 (or 14) digit number that identifies subscribers on GSM/UMTS networks. The IMSI is stored on the subscriber's SIM, and comprises a country code (as defined by ITU E.212), a network code (the network operator), and a unique subscriber number.
- **PDP Context - Packet Data Protocol Context** - A data structure representing the logical association of a station on a GPRS network. The data structure comprises a CID (context identifier), a PDP\_Type (the protocol being used, e.g. IP), an APN (Access Point Name), and optional a PDP\_Addr (PDP Address) to identify the usable address space for the connection. After a PDP Context is constructed, it must be activated.
- **SIM - Subscriber Identity Module** - USIM (Universal SIM) in UMTS. A SIM, also known as a Smart Card, stores unique subscriber information, including subscription and service parameters as well as preferences and settings. SIMs are used by all GSM devices, and allow for a subscriber's identity to move from one GSM device to another. Many operators lock their devices to prevent the use of other operator's SIM cards, but operators will sometimes unlock their devices if certain conditions are met.
- **TDMA - Time Division Multiple Access** - TDMA is used by most currently available GSM networks. It allows multiple concurrent access to a frequency by dividing it into time-slots, where each station takes turns transmitting. Since TDMA based technologies switch their transmitters on and off rapidly (native TDMA switches at 50 Hz, GSM switches at 217 Hz), radio frequency (RF) pollution is created. When the power output is high enough (such as right before a call is received), these RF signals (particularly GSM's 217 Hz signal, which is in the audible spectrum, even on really cheap computer speakers) can be picked up by nearby amplification circuitry, producing a buzzing sound. So don't put your GSM equipped TZ 190 on top of a stereo, and don't balance it on your head if you wear hearing aids.
- **UMTS - Universal Mobile Telecommunication System** - Employing W-CDMA technology, UMTS is considered the evolution of GSM, and is sometimes referred to as 3GSM. UMTS is in fairly wide deployment worldwide, with the exception of the Americas, where EDGE is favored, and where UMTS will likely be leapfrogged as GSM's successor by HSDPA.

- **W-CDMA - Wideband Code Division Multiple Access** - The technology underlying UMTS, W-CDMA is an evolution of the GSM protocol. Referred to a Wideband because its carrier channels are four times wider than then original CDMA standard (5 MHz versus 1.25 MHz).

# **PART 6**

# **SonicPoint**



# CHAPTER 35

## Managing SonicPoints

### SonicPoint > SonicPoints

SonicWALL SonicPoints are wireless access points specially engineered to work with SonicWALL security appliances to provide wireless access throughout your enterprise.

The SonicPoint section of the Management Interface lets you manage the SonicPoints connected to your system.



### Before Managing SonicPoints

Before you can manage SonicPoints in the Management Interface, you must first:

- Verify that the SonicPoint image is downloaded to your SonicWALL security appliance. See [“Updating SonicPoint Firmware” on page 398](#).
- Configure your SonicPoint Provisioning Profiles
- Configure a Wireless zone.
- Assign profiles to wireless zones. This step is optional. If you do not assign a default profile for a zone, SonicPoints in that zone will use the first profile in the list.
- Assign an interface to the Wireless zone.

- Attach the SonicPoints to the interfaces in the Wireless zone.
- Test SonicPoints

## SonicPoint Provisioning Profiles

SonicPoint Provisioning Profiles provide a scalable and highly automated method of configuring and provisioning multiple SonicPoints across a Distributed Wireless Architecture. SonicPoint Profile definitions include all of the settings that can be configured on a SonicPoint, such as radio settings for the 2.4GHz and 5GHz radios, SSID's, and channels of operation.

Once you have defined a SonicPoint profile, you can apply it to a Wireless zone. Each Wireless zone can be configured with one SonicPoint profile. Any profile can apply to any number of zones. Then, when a SonicPoint is connected to a zone, it is automatically provisioned with the profile assigned to that zone.

SonicOS includes a default SonicPoint profile, named SonicPoint. You can modify this profile or create a new one.


The default SonicPoint profile has the following settings:

802.11a Radio		802.11g Radio	
Enable 802.11a Radio	Yes - Always on	Enable 802.11g Radio	Yes - Always on
SSID	SonicWALL	SSID	SonicWALL
Radio Mode	54Mbps - 802.11a	Radio Mode	2.4 GHz 54Mbps - 802.11g
Channel	AutoChannel	Channel	AutoChannel
ACL Enforcement	Disabled	ACL Enforcement	Disabled
Authentication Type	WEP - Both Open System & Shared Key	Authentication Type	WEP - Both Open System & Shared Key
Schedule IDS Scan	Disabled	Schedule IDS Scan	Disabled
Data Rate	Best	Data Rate	Best
Antenna Diversity	Best	Antenna Diversity	Best



## Configuring a SonicPoint Profile

You can add any number of SonicPoint profiles. To configure a SonicPoint provisioning profile:

- Step 1** To add a new profile click **Add** below the list of SonicPoint provisioning profiles. To edit an existing profile, select the profile and click the edit icon  in the same line as the profile you are editing.
- Step 2** In the **General** tab of the Add Profile window, specify:



- **Enable SonicPoint:** Check this to automatically enable each SonicPoint when it is provisioned with this profile.
- **Name Prefix:** Enter a prefix for the names of all SonicPoints connected to this zone. When each SonicPoint is provisioned it is given a name that consists of the name prefix and a unique number, for example: “SonicPoint 126008.”

- **Country Code:** Select the country where you are operating the SonicPoints. The country code determines which regulatory domain the radio operation falls under.

**Step 3** In the **802.11g** tab, Configure the radio settings for the 802.11g (2.4GHz band) radio:

The screenshot shows the 'Add SonicPoint Profile' window in Microsoft Internet Explorer. The '802.11g Radio Settings' tab is active. The 'Enable Radio' checkbox is checked, and the schedule is set to 'Always on'. The SSID field is empty. The 'Radio Mode' is set to '2.4GHz 54Mbps - 802.11g' and the 'Channel' is set to 'AutoChannel'. Under 'ACL Enforcement', the 'Enable MAC Filter List' checkbox is unchecked. The 'Allow List' and 'Deny List' are both set to '-Select an Address Object Group-'. Under 'WEP/WPA Encryption', the 'Authentication Type' is set to 'WEP - Both (Open System & Shared Key)', the 'WEP Key Type' is 'Name', and the 'Default Key' is 'Key 1'. There are four empty text boxes for 'Key 1', 'Key 2', 'Key 3', and 'Key 4'. The status bar at the bottom says 'Ready'.

- **Enable 802.11g Radio:** Check this to automatically enable the 802.11g radio bands on all SonicPoints provisioned with this profile.
- Select a schedule to determine when the radio is enabled. The default is **Always on**. you can create and manage Schedule objects in the **System > Schedules** page of the management interface.
- **SSID:** Enter a recognizable string for the SSID of each SonicPoint using this profile. This is the name that will appear in clients' lists of available wireless connections.



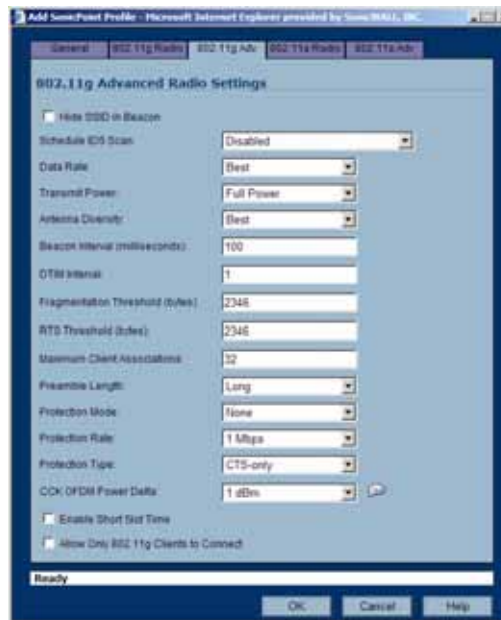
**Note**

If all SonicPoints in your organization share the same SSID, it is easier for users to maintain their wireless connection when roaming from one SonicPoint to another.

- **Radio Mode:** Select the speed of the wireless connection. You can choose **11Mbps - 802.11b**, **54 Mbps - 802.11g**, or **108 Mbps - Turbo G** mode. If you choose Turbo mode, all users in your company must use wireless access cards from the same manufacturer.
- **Channel:** Select the channel the radio will operate on. The default is **AutoChannel**, which automatically selects the channel with the least interference. Use AutoChannel unless you have a specific reason to use or avoid specific channels.
- **ACL Enforcement:** Select this to enforce Access Control by allowing or denying traffic from specific devices. Select a MAC address group from the **Allow List** to automatically allow traffic from all devices with MAC address in the group. Select a MAC address group from the **Deny List** to automatically deny traffic from all devices with MAC address in the group. The deny list is enforced before the Allow list.
- **Authentication Type:** Select the method of authentication for your wireless network. You can select **WEP - Both (Open System & Shared Key)**, **WEP - Open System**, **WEP - Shared Key**, **WPA - PSK**, or **WPA - EAP**.
- **WEP Key Mode:** Select the size of the encryption key.

- **Default Key:** Select which key in the list below is the default key, which will be tried first when trying to authenticate a user.
- **Key Entry:** Select whether the key is alphanumeric or hexadecimal.
- **Key 1 - Key 4:** Enter the encryptions keys for WEP encryption. Enter the most likely to be used in the field you selected as the default key.

**Step 4** In the **802.11g Advanced** tab, configure the performance settings for the 802.11g radio. For most 802.11g advanced options, the default settings give optimum performance.



- **Hide SSID in Beacon:** Check this option to have the SSID broadcast as part of the wireless beacon, rather than as a separate broadcast.
- **Schedule IDS Scan:** Select a time when there are fewer demands on the wireless network to schedule an Intrusion Detection Service (IDS) scan to minimize the inconvenience of dropped wireless connections.
- **Data Rate:** Select the speed at which the data is transmitted and received. **Best** automatically selects the best rate available in your area given interference and other factors. You can select: **Best**, **6 Mbps**, **9 Mbps**, **12 Mbps**, **18 Mbps**, **24 Mbps**, **36 Mbps**, **48 Mbps**, or **54 Mbps**.
- **Transmit Power:** Select the transmission power. Transmission power effects the range of the SonicPoint. You can select: **Full Power**, **Half (-3 dB)**, **Quarter (-6 dB)**, **Eighth (-9 dB)**, or **Minimum**.
- **Antenna Diversity:** The **Antenna Diversity** setting determines which antenna the SonicPoint uses to send and receive data. You can select:
  - **Best:** This is the default setting. When **Best** is selected, the SonicPoint automatically selects the antenna with the strongest, clearest signal. In most cases, **Best** is the optimal setting.
  - **1:** Select **1** to restrict the SonicPoint to use antenna 1 only. Facing the rear of the SonicPoint, antenna 1 is on the left, closest to the power supply.
  - **2:** Select **2** to restrict the SonicPoint to use antenna 2 only. Facing the rear of the SonicPoint, antenna 2 is on the right, closest to the console port.
- **Beacon Interval (milliseconds):** Enter the number of milliseconds between sending out a wireless beacon.

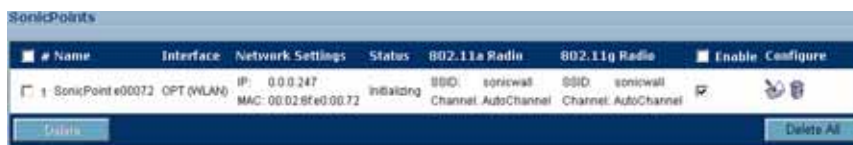
- **DTIM Interval:** Enter the interval in milliseconds.
- **Fragmentation Threshold (bytes):** Enter the number of bytes of fragmented data you want the network to allow.
- **RTS Threshold (bytes):** Enter the number of bytes.
- **Maximum Client Associations:** Enter the maximum number of clients you want the SonicPoint to support on this radio at one time.
- **Preamble Length:** Select the length of the preamble--the initial wireless communication send when associating with a wireless host. You can select **Long** or **Short**.
- **Protection Mode:** Select the CTS or RTS protection. Select **None**, **Always**, or **Auto**. **None** is the default.
- **Protection Rate:** Select the speed for the CTS or RTS protection, **1 Mbps**, **2 Mbps**, **5 Mbps**, or **11 Mbps**.
- **Protection Type:** Select the type of protection, **CTS-only** or **RTS-CTS**.
- **CCK OFDM Power Delta:** Select the difference in radio transmit power you will allow between the 802.11b and 802.11g modes: 0 dBm, 1 dBm, or 2 dBm.
- **Enable Short Slot Time:** Allow clients to disassociate and reassociate more quickly.
- **Allow Only 802.11g Clients to Connect:** Use this if you are using Turbo G mode and therefore are not allowing 802.11b clients to connect.



**Step 5** Configure the settings in the **802.11a Radio** and **802.11a Advanced** tabs. These settings affect the operation of the 802.11a radio bands. The SonicPoint has two separate radios built in. Therefore, it can send and receive on both the 802.11a and 802.11g bands at the same time.

The settings in the **802.11a Radio** and **802.11a Advanced** tabs are similar to the settings in the **802.11g Radio** and **802.11g Advanced** tabs. Follow the instructions in step 3 and step 4 in this procedure to configure the 802.11a radio.

When a SonicPoint unit is first connected and powered up, it will have a factory default configuration (IP Address 192.168.1.20, username: admin, password: password). Upon initializing, it will attempt to find a SonicOS device with which to peer. If it is unable to find a peer SonicOS device, it will enter into a stand-alone mode of operation with a separate stand-alone configuration allowing it to operate as a standard Access Point.

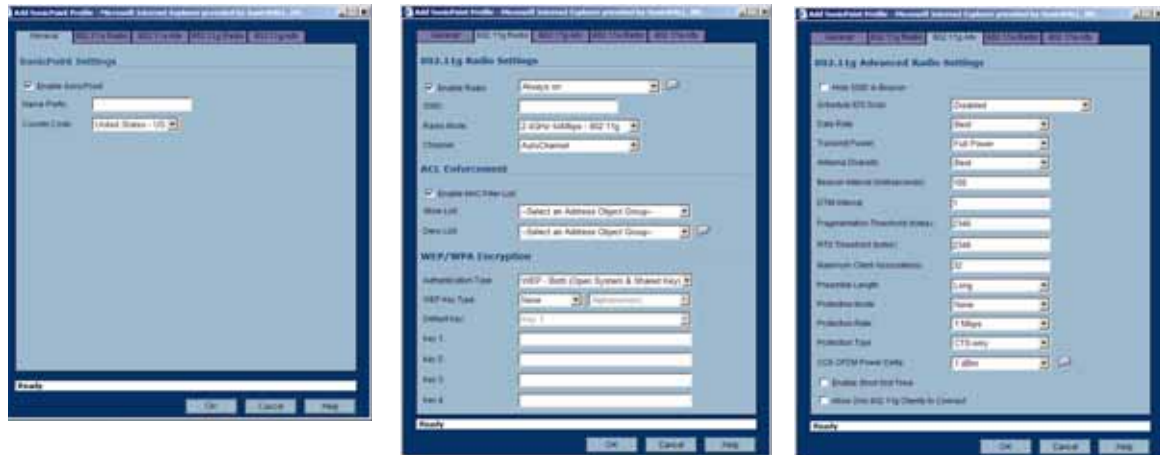
If the SonicPoint does locate, or is located by a peer SonicOS device, via the SonicWALL Discovery Protocol, an encrypted exchange between the two units will ensue wherein the profile assigned to the relevant Wireless Zone will be used to automatically configure (provision) the newly added SonicPoint unit.



#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPoint e0072	OPT (WLAN)	IP: 0.0.0.247 MAC: 00:02:8f:e0:00:72	initializing	SSID: sonicwall Channel: AutoChannel	SSID: sonicwall Channel: AutoChannel	<input type="checkbox"/>	 

As part of the provisioning process, SonicOS will assign the discovered SonicPoint device a unique name, and it will record its MAC address and the interface and Zone on which it was discovered. It can also automatically assign the SonicPoint an IP address, if so configured, so

that the SonicPoint can communicate with an authentication server for WPA-EAP support. SonicOS will then use the profile associated with the relevant Zone to configure the 2.4GHz and 5GHz radio settings.



Modifications to profiles will not affect units that have already been provisioned and are in an operational state. Configuration changes to operational SonicPoint devices can occur in two ways:


- Via manual configuration changes – Appropriate when a single, or a small set of changes are to be affected, particularly when that individual SonicPoint requires settings that are different from the profile assigned to its Zone.
- Via un-provisioning – Deleting a SonicPoint unit effectively un-provisions the unit, or clears its configuration and places it into a state where it will automatically engage the provisioning process anew with its peer SonicOS device. This technique is useful when the profile for a Zone is updated or changed, and the change is set for propagation. It can be used to update firmware on SonicPoints, or to simply and automatically update multiple SonicPoint units in a *controlled* fashion, rather than changing all peered SonicPoints at once, which can cause service disruptions.

## Updating SonicPoint Settings

You can change the settings of any individual SonicPoint list on the **Sonicpoint > SonicPoints** page.

### Edit SonicPoint settings

To edit the settings of an individual SonicPoint:

- Step 1** Under SonicPoint Settings, click the Edit icon  in the same line as the SonicPoint you want to edit.
- Step 2** In Edit SonicPoint screen, make the changes you want. The Edit SonicPoint screen has the following tabs:
  - General
  - 802.11a Radio
  - 802.11a Advanced
  - 802.11g Radio
  - 802.11g Advanced

The options on these tabs are the same as the Add SonicPoint Profile screen. See [Configuring a SonicPoint Profile](#) for instructions on configuring these settings.

**Step 3** Click **OK** to apply these settings.

## Synchronize SonicPoints

Click **Synchronize SonicPoints** at the top of the **SonicPoint > SonicPoints** page to update the settings for each SonicPoint reported on the page. When you click **Synchronize SonicPoints**, SonicOS polls all connected SonicPoints and displays updated settings on the page.

## Enable and Disable Individual SonicPoints

You can enable or disable individual SonicPoints on the **SonicPoint > SonicPoints** page:

**Step 1** Check the box under Enable to enable the SonicPoint, uncheck the box to disable it.



**Step 2** Click **Apply** at the top of the **SonicPoint > SonicPoints** page to apply this setting to the SonicPoint.

## Updating SonicPoint Firmware

SonicOS Enhanced 4.0 does *not* contain an image of the SonicPoint firmware.

If your SonicWALL appliance has Internet connectivity, it will automatically download the correct version of the SonicPoint image from the SonicWALL server when you connect a SonicPoint device.

If your SonicWALL appliance does *not* have Internet access, or has access only through a proxy server, you must perform the following steps:

**Step 1** Download the SonicPoint image from <http://www.mysonicwall.com> to a local system with Internet access.

You can download the SonicPoint image from one of the following locations:

- On the same page where you can download the SonicOS Enhanced firmware
- On the Download Center page, by selecting **SonicPoint** in the Type drop-down menu

**Step 2** Load the SonicPoint image onto a local Web server that is reachable by your SonicWALL appliance.

You can change the file name of the SonicPoint image, but you should keep the .bin extension.

**Step 3** In the SonicOS user interface on your SonicWALL appliance, in the navigation pane, click **System** and then click **Administration**.

**Step 4** In the System > Administration screen, under Download URL, click the **Manually specify SonicPoint image URL** checkbox to enable it.

**Step 5** In the text box, type the URL for the SonicPoint image file on your local Web server.

**Step 6** Click **Apply**.

---

**Caution** *It is imperative that you download the corresponding SonicPoint image for the SonicOS firmware version that is running on your SonicWALL. The mysonicwall.com Web site provides information about the corresponding versions. When upgrading your SonicOS firmware, be sure to upgrade to the correct SonicPoint image.*

---

## Automatic Provisioning (SDP & SSPP)

The SonicWALL Discovery Protocol (SDP) is a layer 2 protocol employed by SonicPoints and devices running SonicOS Enhanced. SDP is the foundation for the automatic provisioning of SonicPoint units via the following messages:

- **Advertisement** – SonicPoint devices without a peer will periodically and on startup announce or advertise themselves via a broadcast. The advertisement will include information that will be used by the receiving SonicOS device to ascertain the state of the SonicPoint. The SonicOS device will then report the state of all peered SonicPoints, and will take configuration actions as needed.
- **Discovery** – SonicOS devices will periodically send discovery request broadcasts to elicit responses from L2 connected SonicPoint units.
- **Configure Directive** – A unicast message from a SonicOS device to a specific SonicPoint unit to establish encryption keys for provisioning, and to set the parameters for and to engage configuration mode.
- **Configure Acknowledgement** – A unicast message from a SonicPoint to its peered SonicOS device acknowledging a Configure Directive.
- **Keepalive** – A unicast message from a SonicPoint to its peered SonicOS device used to validate the state of the SonicPoint.

If via the SDP exchange the SonicOS device ascertains that the SonicPoint requires provisioning or a configuration update (e.g. on calculating a checksum mismatch, or when a firmware update is available), the Configure directive will engage a 3DES encrypted, reliable TCP based SonicWALL Simple Provisioning Protocol (SSPP) channel. The SonicOS device will then send the update to the SonicPoint via this channel, and the SonicPoint will restart with the updated configuration. State information will be provided by the SonicPoint, and will be viewable on the SonicOS device throughout the entire discovery and provisioning process.

## SonicPoint States

SonicPoint devices can function in and report the following states:

- **Initializing** – The state when a SonicPoint starts up and advertises itself via SDP prior to it entering into an operational or stand-alone mode.

- **Operational** – Once the SonicPoint has peered with a SonicOS device and has its configuration validated, it will enter into a operational state, and will be ready for clients.
- **Provisioning** – If the SonicPoint configuration requires an update, the SonicOS device will engage an SSPP channel to update the SonicPoint. During this brief process it will enter the provisioning state.
- **Safemode** – Safemode can be engaged by depressing the reset button, or from the SonicOS peer device. Placing a SonicPoint into Safemode returns its configuration to defaults, disables the radios, and disables SDP. The SonicPoint must then be rebooted to enter either a stand-alone, or some other functional state.
- **Non-Responsive** – If a SonicOS device loses communications with a previously peered SonicPoint, it will report its state as non-responsive. It will remain in this state until either communications are restored, or the SonicPoint is deleted from the SonicOS device's table.
- **Updating Firmware** – If the SonicOS device detects that it has a firmware update available for a SonicPoint, it will use SSPP to update the SonicPoint's firmware.
- **Over-Limit** – By default, up to 2 SonicPoint devices can be attached to the Wireless Zone interface on a SonicWALL TZ 170. If more than 2 units are detected, the over-limit devices will report an over-limit state, and will not enter an operational mode. The number can be reduced from 2 as needed.
- **Rebooting** – After a firmware or configuration update, the SonicPoint will announce that it is about to reboot, and will then do so.
- **Firmware failed** – If a firmware update fails, the SonicPoint will report the failure, and will then reboot.
- **Provision failed** – In the unlikely event that a provision attempt from a SonicOS device fails, the SonicPoint will report the failure. So as not to enter into an endless loop, it can then be manually rebooted, manually reconfigured, or deleted and re-provisioned.
- **Stand-alone Mode (not reported)** – If a SonicPoint device cannot find or be found by a SonicOS device to peer with, it will enter a stand-alone mode of operation. This will engage the SonicPoint's internal GUI (which is otherwise disabled) and will allow it to be configured as a conventional Access Point. If at any time it is placed on the same layer 2 segment as a SonicOS device that is sending Discovery packets, it will leave stand-alone mode, and will enter into a managed mode. The stand-alone configuration will be retained.



# CHAPTER 36

## Viewing Station Status

### SonicPoint > Station Status

The **SonicPoint > Station Status** page reports on the statistics of each SonicPoint.








The screenshot shows the 'SonicPoint > Station Status' page. At the top right is a 'Refresh' button. Below the title, there is a 'Station Status' section with a 'Items' dropdown set to '2 (of 2)'. A 'View Style' dropdown is set to 'SonicPoint' and a filter dropdown is set to 'All SonicPoints'. The main content is a table with the following data:

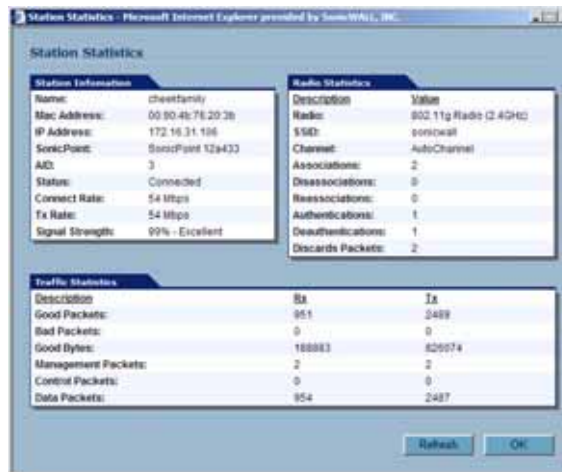
#	SonicPoint	Station	MAC Address	Status	Type	SSID	AID	Connect Rate	Tx Rate	Signal Strength	Statistics
SonicPoint e00072 - Status was updated 00:00:03 ago											
1	SonicPoint e00072		00:02:ef:20:be:29	Connected	50Hz	1_sonicwall	1	54 Mbps	8 Mbps	76% - Very Good	
2	SonicPoint e00072	172.16.32.2	00:90:4b:76:20:3b	Connected	2.40Hz	1_sonicwall	1	1 Mbps	48 Mbps	100% - Excellent	

The table lists entries for each wireless client connected to each SonicPoint. The sections of the table are divided by SonicPoint. Under each SonicPoint, is the list of all clients currently connected to it.

Click the **Refresh** button in the top right corner to refresh the list.

By default, the page displays the first 50 entries found. Click the First Page , Previous Page , Next Page , and Last Page  icons to navigate if you need to view more than 50 entries.

Click on the Statistics icon  to see a detailed report for an individual station. Each SonicPoint device reports for both radios, and for each station, the following information to its SonicOS peer:



Station Information		Radio Statistics	
Name:	cheetah	Description:	3088
Mac Address:	00 90 4b 76 20 2b	Radio:	802.11g Radio (2.4GHz)
IP Address:	172.16.31.106	SSID:	sonicwall
SonicPoint:	SonicPoint 128433	Channel:	AutoChannel
AID:	3	Associations:	2
Status:	Connected	Disassociations:	0
Connect Rate:	54 Mbps	Reassociations:	0
Tx Rate:	54 Mbps	Authentications:	1
Signal Strength:	99% - Excellent	Deauthentications:	1
		Discards Packets:	2

Traffic Statistics		
Description	Rx	Tx
Good Packets:	951	2489
Bad Packets:	0	0
Good Bytes:	188883	82074
Management Packets:	2	2
Control Packets:	0	0
Data Packets:	954	2487

- MAC Address – The client's (Station's) hardware address.
- Station State – The state of the station. States can include:
  - None – No state information yet exists for the station.
  - Authenticated – The station has successfully authenticated.
  - Associated – The station is associated.
  - Joined – The station has joined the ESSID.
  - Connected – The station is connected (joined, authenticated or associated).
  - Up – An Access Point state, indicating that the Access Point is up and running.
  - Down – An Access Point state, indicating that the Access Point is not running.
- Associations – Total number of Associations since power up.
- Dis-Associations – Total number of Dis-Associations.
- Re-Associations – Total number of Re-Associations.
- Authentications – Number of Authentications.
- De-Authentications – Number of De-Authentications.
- Good Frames Received – Total number of good frames received.
- Good Frames Transmitted – Total number of good frames transmitted.
- Error in Receive Frames – Total number of error frames received.
- Error in Transmit Frames – Total number of error frames transmitted.
- Discarded Frames – Total number of frames discarded. Discarded frames are generally a sign of network congestion.
- Total Bytes received – Total number of bytes received.
- Total Bytes Transmitted – Total number of bytes transmitted.
- Management Frames Received – Total number of Management frames received. Management Frames include:
  - Association request
  - Association response

- Re-association request
- Re-association response
- Probe request
- Probe response
- Beacon frame
- ATIM message
- Disassociation
- Authentication
- De-authentication
- Management Frames Transmitted – Total number of Management frames transmitted.
- Control Frames Received – Total number of Control frames received. Control frames include:
  - RTS – Request to Send
  - CTS – Clear to Send
  - ACK – Positive Acknowledgement
- Control Frames Transmitted – Total number of Control frames transmitted.
- Data Frames Received – Total number of Data frames received.
- Data Frames Transmitted – Total number of Data frames transmitted.



# CHAPTER 37

## Using and Configuring IDS

### SonicPoint > IDS

You can have many wireless access points within reach of the signal of the SonicPoints on your network. The **SonicPoint > IDS** page reports on all access points the SonicWALL security appliance can find by scanning the 802.11a and 802.11g radio bands.

#	SonicPoint	MAC Address (BSSID)	SSID	Type	Channel	Manufacturer	Signal Strength	Max Rate	Authorize
SonicPoint e00072 - The last scan was performed 1 Day 01:31:06 ago									
1	SonicPoint e00072	00:06:b1:12:71:5a	SWBETA	5GHz	56	SonicWALL	39% - Fair	54 Mbps	
2	SonicPoint e00072	00:02:8f:2e:21:f9	sonicwall	5GHz	58	Senao	60% - Very Good	54 Mbps	
3	SonicPoint e00072	00:02:8f:2e:21:df	sonicwall	5GHz	60	Senao	78% - Very Good	54 Mbps	
4	SonicPoint e00072	00:02:8f:2e:20:cd	Atheros Wireless Network	5GHz	60	Senao	60% - Very Good	54 Mbps	
5	SonicPoint e00072	00:02:8f:2e:20:bf	csiwqalPRO2040SPa	5GHz	64	Senao	78% - Very Good	54 Mbps	
6	SonicPoint e00072	00:02:8f:2e:21:f1	sonicwall	5GHz	64	Senao	39% - Fair	54 Mbps	
7	SonicPoint e00072	00:0d:8c:6c:4f:26	olivea	5GHz	36	Cisco	39% - Fair	54 Mbps	
8	SonicPoint e00072	00:02:8f:2e:21:cb	sonicwall	5GHz	38	Senao	60% - Very Good	54 Mbps	
9	SonicPoint e00072	00:06:b1:12:71:94	sonicwall	5GHz	40	SonicWALL	78% - Very Good	54 Mbps	

### Wireless Intrusion Detection Services

Intrusion Detection Services (IDS) greatly increase the security capabilities of the SonicWALL security appliance with SonicOS Enhanced by enabling it to recognize and even take countermeasures against the most common types of illicit wireless activity. IDS consists of three types of services, namely, Sequence Number Analysis, Association Flood Detection, and Rogue Access Point Detection. IDS logging and notification can be enabled under **Log > Categories** by selecting the **IDS** checkbox under **Log Categories** and **Alerts**.

## Intrusion Detection Settings

Rogue Access Points have emerged as one of the most serious and insidious threats to wireless security. In general terms, an access point is considered rogue when it has not been authorized for use on a network. The convenience, affordability and availability of non-secure access points, and the ease with which they can be added to a network creates a easy environment for introducing rogue access points. Specifically, the real threat emerges in a number of different ways, including unintentional and unwitting connections to the rogue device, transmission of sensitive data over non-secure channels, and unwanted access to LAN resources. So while this doesn't represent a deficiency in the security of a specific wireless device, it is a weakness to the overall security of wireless networks.

The security appliance can alleviate this weakness by recognizing rogue access points potentially attempting to gain access to your network. It accomplishes this in two ways: active scanning for access points on all 802.11a and 802.11g channels, and passive scanning (while in Access Point mode) for beaconing access points on a single channel of operation.

Check **Enable Rogue Access Point Detection** to enable the security appliance to search for rogue access points.

The **Authorized Access Points** list determines which access points the security appliance will considered authorized when it performs a scan. You can select **All Authorized Access Points** to allow all SonicPoints, or you can select an address object group containing a group of MAC address to limit the list to only those SonicPoints whose MAC addresses are contained in the address object group.

Select Create Address Object Group to add a new group of MAC address objects to the list.



**Note** See "[Network > Address Objects](#)" section on page 203 for instructions on creating address objects and address object groups.

## Scanning for Access Points

Active scanning occurs when the security appliance starts up, and at any time **Scan All** is clicked on the **SonicPoint > IDS** page. When the security appliance performs a scan, a temporary interruption of wireless clients occurs for no more than a few seconds. This interruption manifests itself as follows:

- Non-persistent, stateless protocols (such as HTTP) should not exhibit any ill-effects.
- Persistent connections (protocols such as FTP) are impaired or severed.
- WiFiSec connections should automatically re-establish and resume with no noticeable interruption to the client.

**Caution** If service disruption is a concern, it is recommended that the Scan Now feature not be used while the SonicWALL security appliance is in Access Point mode until such a time that no clients are active, or the potential for disruption becomes acceptable.

You can also scan on a SonicPoint by SonicPoint basis by choosing from the following options in the Perform SonicWALL Scan menu on the header for the individual SonicPoint:

- Scan Both Radios
- Scan 802.11a Radio (5GHz)
- Scan 802.11g Radio (2.4GHZ)

## Discovered Access Points

The Discovered Access points displays information on every access point that can be detected by the SonicPoint radio:

- **SonicPoint:** The SonicPoint that detected the access point.
- **MAC Address (BSSID):** The MAC address of the radio interface of the detected access point.
- **SSID:** The radio SSID of the access point.
- **Type:** The range of radio bands used by the access point, 2.4 GHz or 5 GHz.
- **Channel:** The radio channel used by the access point.
- **Manufacturer:** The manufacturer of the access point. SonicPoints will show a manufacturer of either *SonicWALL* or *Senaos*.
- **Signal Strength:** The strength of the detected radio signal
- **Max Rate:** The fastest allowable data rate for the access point radio, typically 54 Mbps.
- **Authorize:** Click the Authorize icon to add the access point to the address object group of authorized access points.

### View Style

If you have more than one SonicPoint, you can select an individual device from the **SonicPoint** list to limit the **Discovered Access Points** table to display only scan results from that SonicPoint. Select **All SonicPoints** to display scan results from all SonicPoints.



## Authorizing Access Points on Your Network

Access Points detected by the security appliance are regarded as rogues until they are identified to the security appliance as authorized for operation. To authorize an access point, it can be manually added to the **Authorized Access Points** list by clicking edit icon in the **Authorize** column and specifying its MAC address (BSSID) along with an optional comment. Alternatively, if an access point is discovered by the security appliance scanning feature, it can be added to the list by clicking the **Authorize** icon.







## CHAPTER 38

# Configuring RF Monitoring

---

## SonicPoint > RF Monitoring

This chapter describes how to plan, design, implement, and maintain the RF Monitoring feature in SonicWALL SonicOS 4.0 Enhanced. This chapter contains the following sections:

- [“RF Monitoring Overview” section on page 409](#)
  - [“Why RF Monitoring?” section on page 410](#)
  - [“Benefits” section on page 410](#)
- [“Enabling RF Monitoring on SonicPoint\(s\)” section on page 411](#)
- [“Using The RF Monitoring Interface” section on page 411](#)
  - [“Selecting RF Signature Types” section on page 412](#)
  - [“Viewing Discovered RF Threat Stations” section on page 413](#)
  - [“Adding a Threat Station to the Watch List” section on page 413](#)
- [“Types of RF Threat Detection” section on page 414](#)
- [“Practical RF Monitoring Field Applications” section on page 415](#)
  - [“Before Reading this Section” section on page 415](#)
  - [“Using Sensor ID to Determine RF Threat Location” section on page 415](#)
  - [“Using RSSI to Determine RF Threat Proximity” section on page 417](#)

## RF Monitoring Overview

The following section provides a brief overview of the RF Monitoring feature found on SonicWALL security appliances running SonicOS 4.0 or higher. This section contains the following subsections:

- [“Why RF Monitoring?” section on page 410](#)
- [“Benefits” section on page 410](#)

## Why RF Monitoring?

Radio Frequency (RF) technology used in today's 802.11-based wireless networking devices poses an attractive target for intruders. If left un-managed, RF devices can leave your wireless (and wired) network open to a variety of outside threats, from Denial of Service (DoS) to network security breaches.

In order to help secure your SonicPoint Wireless Access Point (AP) stations, SonicWALL takes a closer look at these threats. By using direct RF Monitoring, SonicWALL helps detect threats without interrupting the current operation of your wireless or wired network.

## Benefits

SonicWALL RF Monitoring provides real-time threat monitoring and management of SonicPoint radio frequency traffic. In addition to its real-time threat management capabilities, SonicWALL RF Monitoring provides network administrators a system for centralized collection of RF threats and traffic statistics; offering a way to easily manage RF capabilities directly from the SonicWALL security appliance gateway

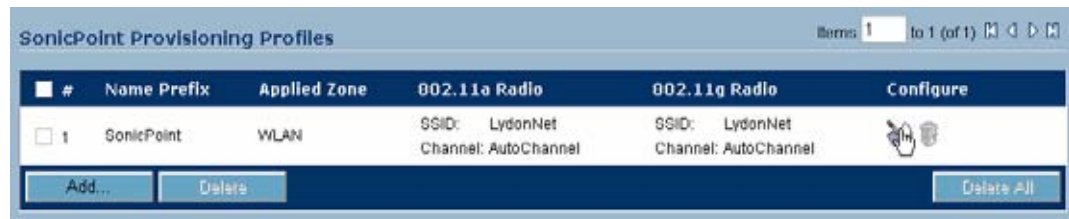
SonicWALL RF Monitoring is:

- **Real-Time** - View logged information as it happens
- **Transparent** - No need to halt legitimate network traffic when managing threats
- **Comprehensive** - Provides detection of many types of RF threats. For complete descriptions of the above types of RF Threat Detection, see the ["Types of RF Threat Detection" section on page 414](#).

## Enabling RF Monitoring on SonicPoint(s)

In order for RF Monitoring to be enforced, you must enable the RF Monitoring option on all available SonicPoint devices. The following section provides instructions to re-provision all available SonicPoints with RF Monitoring enabled.

- Step 1** Navigate to **SonicPoint > SonicPoints** in the SonicWALL security appliance management interface.
- Step 2** Click the **Configure** button corresponding to the desired SonicPoint Provisioning Profile.



- Step 3** In the **General** tab, click the **Enable RF Monitoring** checkbox.



Next, to ensure all SonicPoints are updated with the RF Monitoring feature enabled, it is necessary to delete all current SonicPoints from the SonicPoint table and re-synchronize these SonicPoints using the profile you just created.

- Step 4** Click the **Delete All** button at the bottom right corner of the SonicPoints table.
- Step 5** Click the **Synchronize SonicPoints** button at the top of the page.

Your SonicPoints will now reboot with the RF Monitoring feature enabled. Be patient as the reboot process may take several minutes.

## Using The RF Monitoring Interface

The RF Monitoring interface (**SonicPoint > RF Monitoring**) provides a central location for selecting RF signature types, viewing discovered RF threat stations, and adding discovered threat stations to a watch list. This section provides an overview of usage and features for the following RF Monitoring operations:

- [“RF Monitoring Interface Overview” section on page 412](#)
- [“Set the Measurement Interval” section on page 412](#)
- [“Selecting RF Signature Types” section on page 412](#)
- [“Viewing Discovered RF Threat Stations” section on page 413](#)
- [“Adding a Threat Station to the Watch List” section on page 413](#)

## RF Monitoring Interface Overview

The top portion of the RF Monitoring interface allows you to:

- View the number of threats logged for each group/signature
- Select which RF signature types your SonicWALL looks for

The bottom (Discovered RF Threat Stations) portion of the interface allows you to:

- View a detailed log of the most current threats
- Configure a watch list for discovered stations

The screenshot displays the SonicPoint RF Monitoring interface. At the top, there are buttons for Refresh, Clear Stats, Apply, and Cancel. The interface is divided into several sections:

- RF Monitoring Summary:** Shows SonicPoint RF monitoring units: 1, Total RF Threats: 46963, and Measurement Interval (seconds): 300.
- 802.11 General Frame Setting:** Shows Total General Threats: 4450 and Long Duration: 4450 (checked).
- 802.11 Management Frame Setting:** Shows Total Management Threats: 1555 and various threat types with counts and checkboxes: Management Frame Flood (398), Null Probe Response (83), Broadcasting Deauthentication (1068), Valid Station with Invalid SSID (6), Wellenreiter Detection (0), and Ad Hoc Station Detection (0).
- 802.11 Data Frame Setting:** Shows Total Data Threats: 40950 and various threat types with counts and checkboxes: Unassociated Station (40956), NetStumbler Detection (0), EAPOL Packet Flood (0), and Weak WEP IV (2).
- Discovered RF threat stations:** A table listing discovered stations with columns for #, MAC Address, Type, Vendor, Rssi, Rate, Encrypt, RF Threat, Update Time, Sensor, Comment, and Configure.

#	MAC Address	Type	Vendor	Rssi	Rate	Encrypt	RF Threat	Update Time	Sensor	Comment	Configure
1	00:02:8f:01:7e:fa	2.4GHz	Senao	14	2	None	UnAsso Client	10/09/2006 12:16:32	8P 126041		
2	00:02:8f:20:67:07	2.4GHz	Senao	24	1	None	Long Dur	10/09/2006 12:51:02	8P 126041		

### Set the Measurement Interval

In the RF Monitoring Summary section, the **Measurement Interval** field specifies how often the SonicWALL security appliance searches for RF threats. The default is 300 seconds (5 hours).

### Selecting RF Signature Types

The RF Monitoring interface allows you to select which types of RF threats your SonicWALL monitors and logs.

- Step 1** Navigate to **SonicPoint > RF Monitoring** in the SonicWALL security appliance management interface. RF threat types are displayed, with a checkbox next to each.
- Step 2** Click the checkbox next to the RF threat to enable/disable management of that threat. By default, all RF threats are checked as managed.

<input checked="" type="checkbox"/>	Null Probe Response	83
<input checked="" type="checkbox"/>	Broadcasting Deauthentication	1252
<input checked="" type="checkbox"/>	Valid Station with invalid SSID	13

**Tip**

For a complete list of RF Threat types and their descriptions, see the [“Types of RF Threat Detection” section on page 414](#) of this document.

## Viewing Discovered RF Threat Stations

The RF Monitoring Discovered Threat Stations list allows you to view, sort and manage a list of the most recent threats to your wireless network.

#	MAC Address	Type	Vendor	Rssi	Rate	Encrypt	RF Threat	Update Time	Sensor	Comment	Configure
1	00:02:8f:01:7e:fa	2.4GHz	Senao	14	2	None	UnAsso Client	10/09/2006 12:16:32	SP 126041		  

Each logged threat contains (and can be sorted by) the following information:

Log Data	Description
MAC Address	Physical address of the RF threat station.
Type	Type of wireless signal received from the threat station.
Vendor	Manufacturer of the threat station (determined by MAC address).
Rssi	Received signal strength as reported by the SonicPoint. This entry, along with the “sensor” entry, can be helpful in triangulating the actual physical position of the RF threat device.
Rate	Transfer rate (Mbps) of the threat station.
Encrypt	Wireless signal encryption on the threat station, “None” or “Encrypted”.
RF Threat	RF Threat type. For a complete list with descriptions, see the <a href="#">“Types of RF Threat Detection” section on page 414</a> .
Update Time	Time this log record was created/updated.
Sensor	ID of the SonicPoint which recorded this threat. This entry, along with the “Rssi” entry, can be helpful in triangulating the actual physical position of the RF threat device.

**Tip**

**Did you know?** It is possible to find approximate locations of RF Threat devices by using logged threat statistics. For more practical tips and information on using the RF Monitoring threat statistics, see the [“Practical RF Monitoring Field Applications” section on page 415](#)

## Adding a Threat Station to the Watch List

The RF Monitoring Discovered Threat Stations “Watch List” feature allows you to create a watch list of threats to your wireless network. The watch list is used to filter results in the Discovered RF Threat Stations list.


To add a station to the watch list:

**Step 1** In the **SonicPoint > RF Monitoring** page, navigate to the **Discovered RF threat stations** section.

**Step 2** Click the  icon that corresponds to the threat station you wish to add to the watch list.



**Step 3** A confirmation screen will appear. Click **OK** to add the station to the watch list.

**Step 4** If you have accidentally added a station to the watch list, or would otherwise like a station removed from the list, click the  icon that corresponds to the threat station you wish to remove.



**Tip**

Once you have added one or more stations to the watch list, you can filter results to see only these stations in the real-time log by choosing “Only Stations in Watch List Group” from the **View Type** drop-down list.



## Types of RF Threat Detection

The following is a partial list containing descriptions for the most prominent types of RF signatures detected by SonicWALL RF Monitoring:

- **Long Duration Attacks** - Wireless devices share airwaves by dividing the RF spectrum into 14 staggered channels. Each device reserves a channel for a specified (short) duration and during the time that any one device has a channel reserved, other devices know not to broadcast on this channel. Long Duration attacks exploit this process by reserving many RF channels for very long durations, effectively stopping legitimate wireless traffic from finding an open broadcast channel.
- **Management Frame Flood** - This variation on the DoS attack attempts to flood wireless access points with management frames (such as association or authentication requests) filling the management table with bogus requests.
- **Null Probe Response** - When a wireless client sends out a probe request, the attacker sends back a response with a Null SSID. This response causes many popular wireless cards and devices to stop responding.
- **Broadcasting De-Authentication** - This DoS variation sends a flood of spoofed de-authentication frames to wireless clients, forcing them to constantly de-authenticate and subsequently re-authenticate with an access point.
- **Valid Station with Invalid (B)SSID** - In this attack, a rogue access point attempts to broadcast a trusted station ID (ESSID). Although the BSSID is often invalid, the station can still appear to clients as though it is a trusted access point. The goal of this attack is often to gain authentication information from a trusted client.
- **Wellenreiter/NetStumbler Detection** - Wellenreiter and NetStumbler are two popular software applications used by attackers to retrieve information from surrounding wireless networks.

- **Ad-Hoc Station Detection** - Ad-Hoc stations are nodes which provide access to wireless clients by acting as a bridge between the actual access point and the user. Wireless users are often tricked into connecting to an Ad-Hoc station instead of the actual access point, as they may have the same SSID. This allows the Ad-Hoc station to intercept any wireless traffic that connected clients send to or receive from the access point.
- **Unassociated Station** - Because a wireless station attempts to authenticate prior to associating with an access point, the unassociated station can create a DoS by sending a flood of authentication requests to the access point while still unassociated.
- **EAPOL Packet Flood** - Extensible Authentication Protocol over LAN (EAPOL) packets are used in WPA and WPA2 authentication mechanisms. Since these packets, like other authentication request packets, are received openly by wireless access points, a flood of these packets can result in DoS to your wireless network.
- **Weak WEP IV** - WEP security mechanism uses your WEP key along with a randomly chosen 24-bit number known as an Initialization Vector (IV) to encrypt data. Network attackers often target this type of encryption because some of the random IV numbers are weaker than others, making it easier to decrypt your WEP key.

## Practical RF Monitoring Field Applications

This section provides an overview of practical uses for collected RF Monitoring data in detecting Wi-Fi threat sources. Practical RF Monitoring Field Applications are provided as general common-sense suggestions for using RF Monitoring data.

This section contains the following sub-sections:

- [“Before Reading this Section” section on page 415](#)
- [“Using Sensor ID to Determine RF Threat Location” section on page 415](#)
- [“Using RSSI to Determine RF Threat Proximity” section on page 417](#)

### Before Reading this Section

When using RF data to locate threats, keep in mind that wireless signals are affected by many factors. Before continuing, take note of the following:

- **Signal strength is not always a good indicator of distance** - Obstructions such as walls, wireless interference, device power output, and even ambient humidity and temperature can affect the signal strength of a wireless device.
- **A MAC Address is not always permanent** - While a MAC address is generally a good indicator of device type and manufacturer, this address is susceptible to change and can be spoofed. Likewise, originators of RF threats may have more than one hardware device at their disposal.

### Using Sensor ID to Determine RF Threat Location

In the Discovered RF Threat Stations list, the Sensor field indicates which Sonic Point is detecting the particular threat. Using the sensor ID and MAC address of the SonicPoint allows you to easily determine the location of the SonicPoint that is detecting the threat.

**Timesaver**

For this section in particular (and as a good habit in general), you may find it helpful to keep a record of the locations and MAC addresses of your SonicPoint devices.

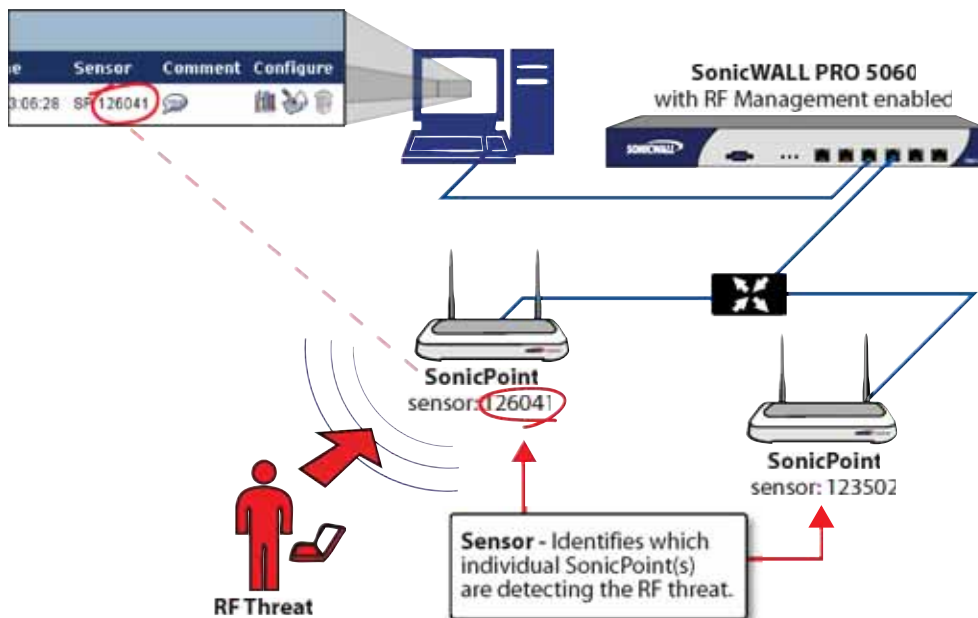
- Step 1** Navigate to the **SonicPoint > RF Monitoring** page in the SonicWALL Management Interface.
- Step 2** In the **Discovered RF Threat Stations** table, locate the **Sensor** for the SonicPoint that is detecting the targeted RF threat and record the number.

#	MAC Address	Type	Vendor	Rssi	Rate	Encrypt	RF Threat	Update Time	Sensor	Comment	Configure
1	00:05:5d:fa:82:b4	2.4GHz	D-Link	7	1	None	UnAuth Client	11/06/2006 13:06:28	SF 126041		

- Step 3** Navigate to **SonicPoint > SonicPoints**.
- Step 4** In the **SonicPoints** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.
- Step 5** Record the **MAC address** for this SonicPoint and use it to find the physical location of the SonicPoint.

#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPoint 126041 X3 (WLAN)		IP: 192.168.0.340 MAC: 00:06:b1:12:60:41	Operational	N/A			

The RF threat is likely to be in the location that is served by this SonicPoint.





## Using RSSI to Determine RF Threat Proximity

This section builds on what was learned in the [“Using Sensor ID to Determine RF Threat Location” section on page 415](#). In the Discovered RF Threat Stations list, the Rssi field indicates the signal strength at which a particular Sonic Point is detecting an RF threat.

The Rssi field allows you to easily determine the proximity of an RF threat to the SonicPoint that is detecting that threat. A higher Rssi number generally means the threat is closer to the SonicPoint.



### Tip

It is important to remember that walls serve as barriers for wireless signals. While a very weak Rssi signal may mean the RF threat is located very far from the SonicPoint, it may also indicate a threat located near, but outside the room or building.

- Step 1** Navigate to the **SonicPoint > RF Monitoring** page in the SonicWALL Management Interface.
- Step 2** In the **Discovered RF Threat Stations** table, locate the **Sensor** and **Rssi** for the SonicPoint that is detecting the targeted RF threat and record these numbers.

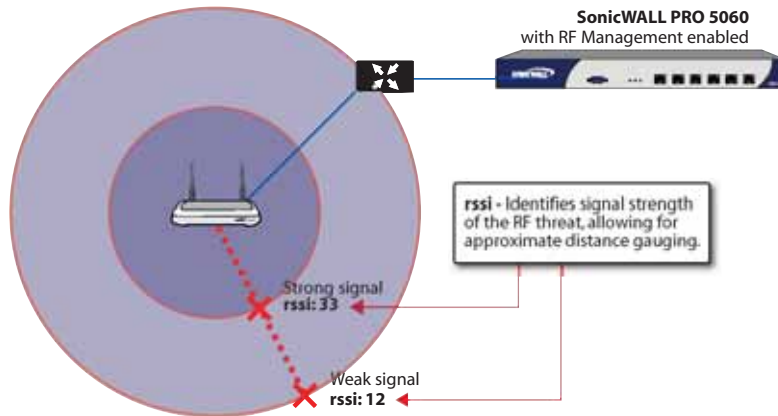
#	MAC Address	Type	Vendor	Rssi	Rate	Encrypt	RF Threat	Update Time	Sensor	Comment	Configure
1	00:05:5d:fa:82:b4	2.4GHz	D-Link	7	1	None	UnAssoc Client	11/06/2008 13:06:28	126041		

- Step 3** Navigate to the **SonicPoint > SonicPoints** page.
- Step 4** In the **SonicPoints** table, locate the SonicPoint that matches the Sensor number you recorded in Step 2.
- Step 5** Record the **MAC address** for this SonicPoint and use it to find the physical location of the SonicPoint.

#	Name	Interface	Network Settings	Status	802.11a Radio	802.11g Radio	Enable	Configure
1	SonicPoint 126041	x3 (WLAN)	IP: 192.168.0.240 MAC: 00:06:b1:12:60:41	Operational	N/A	SSID: Watuhet Channel: AutoChannel Radio: Enabled (Active)	<input checked="" type="checkbox"/>	

A high Rssi usually indicates an RF threat that is closer to the SonicPoint. A low Rssi can indicate obstructions or a more distant RF threat.

20



# **PART 7**

# **Firewall**



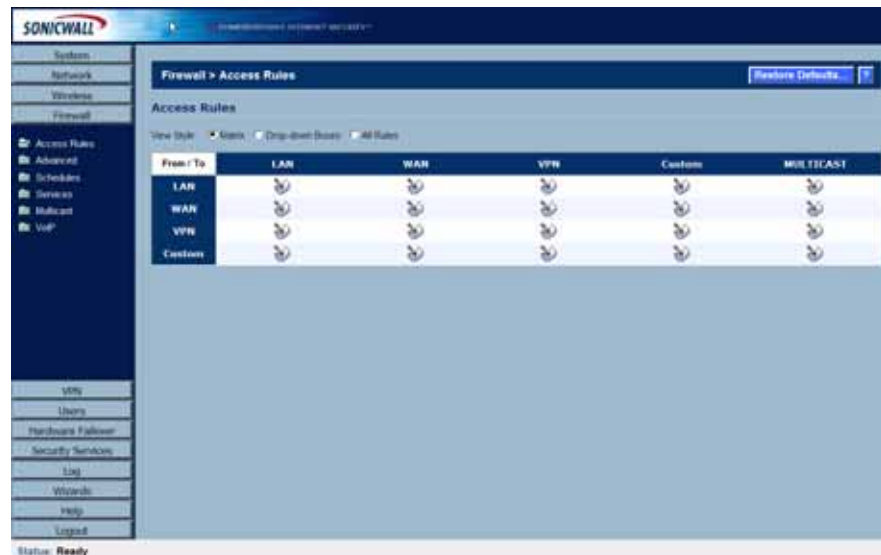
# CHAPTER 39

## Configuring Access Rules

### Firewall > Access Rules

This chapter provides an overview on your SonicWALL security appliance stateful packet inspection default access rules and configuration examples to customize your access rules to meet your business requirements.

Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL security appliance.



The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.

## Stateful Packet Inspection Default Access Rules Overview

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet. The following behaviors are defined by the "Default" stateful inspection packet access rule enabled in the SonicWALL security appliance:

- Allow all sessions originating from the LAN, WLAN to the WAN, DMZ, or OPT.
- Allow all sessions originating from the DMZ or OPT to the WAN.
- Deny all sessions originating from the WAN to the DMZ or OPT.
- Deny all sessions originating from the WAN and DMZ or OPT to the LAN or WLAN.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.

Custom access rules evaluate network traffic source IP addresses, destination IP addresses, IP protocol types, and compare the information to access rules created on the SonicWALL security appliance. Network access rules take precedence, and can override the SonicWALL security appliance's stateful packet inspection. For example, an access rule that blocks IRC traffic takes precedence over the SonicWALL security appliance default setting of allowing this type of traffic.

---

**Caution** The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

---

## Using Bandwidth Management with Access Rules Overview

Bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. All other packets will be queued in the default queue and will be sent in a First In and First Out (FIFO) manner (a storage method that retrieves the item stored for the longest time).

### Example Scenario

If you create an access rule for outbound mail traffic (such as SMTP) and enable bandwidth management with the following parameters:

- Guaranteed bandwidth of 20 percent
- Maximum bandwidth of 40 percent
- Priority of 0 (zero)

The outbound SMTP traffic is guaranteed 20 percent of available bandwidth available to it and can get as much as 40 percent of available bandwidth. If this is the only access rule using bandwidth management, it has priority over all other access rules on the SonicWALL security appliance. Other access rules use the remaining bandwidth (minus 20 percent of bandwidth, or greater than minus 20 percent and less than minus 40 percent of bandwidth).

**Note**

**Note:** Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.

**Tip**

You must select Bandwidth Management on the **WAN > Ethernet** page. Click **Network**, then **Configure** in the **WAN** line of the **Interfaces** table, and type your available bandwidth in the **Available WAN Bandwidth (Kbps)** field.


## Configuration Task List

This section provides a list of the following configuration tasks:

- [“Displaying Access Rules with View Styles” section on page 423](#)
- [“Configuring Access Rules for a Zone” section on page 424](#)
- [“Adding Access Rules” section on page 426](#)
- [“Editing an Access Rule” section on page 429](#)
- [“Deleting an Access Rule” section on page 429](#)
- [“Enabling and Disabling an Access Rule” section on page 429](#)
- [“Restoring Access Rules to Default Zone Settings” section on page 429](#)
- [“Displaying Access Rule Traffic Statistics” section on page 429](#)
- [“Connection Limiting Overview” section on page 429](#)
- [“Access Rule Configuration Examples” section on page 430](#)

## Displaying Access Rules with View Styles

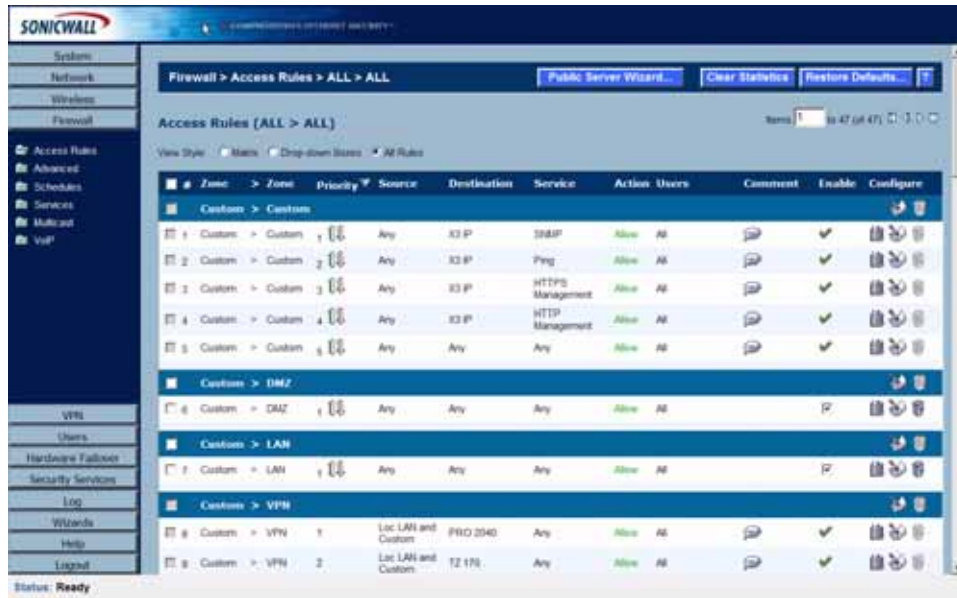
Access rules can be displayed in multiple views using SonicOS Enhanced. You can select the type of view from the selections in the **View Style** section. The following **View Styles** are available:

- **All Rules** - Select **All Rules** to display all access rules configured on the SonicWALL security appliance.
- **Matrix** - Displays as **From/To** with **LAN, WAN, VPN**, or other interface in the **From** row, and **LAN, WAN, VPN**, or other interface in the **To** column. Select the **Edit** icon  in the table cell to view the access rules.
- **Drop-down Boxes** - Displays two pull-down menus: **From Zone** and **To Zone**. Select an interface from the **From Zone** menu and select an interface from the **To Zone** menu. Click **OK** and access rules defined for the two interfaces are displayed.



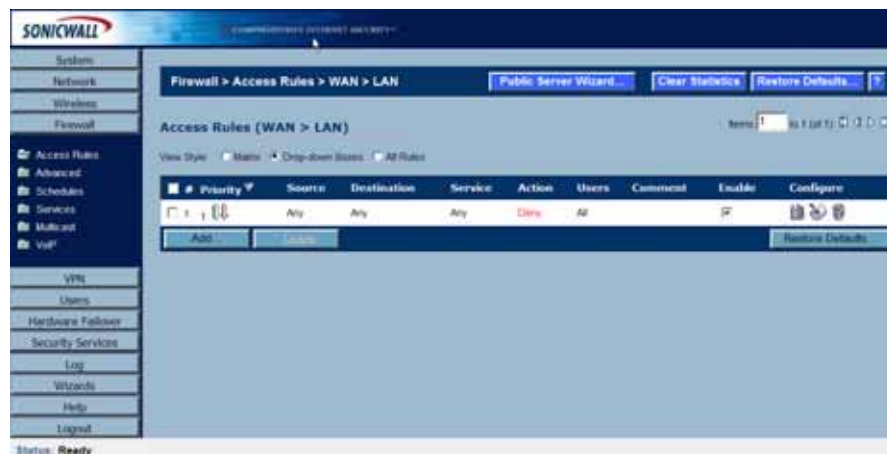
**Tip** You can also view access rules by Zones. Use the Option checkboxes in the **From Zone** and **To Zone** column. Select **LAN**, **WAN**, **VPN**, **ALL** from the **From Zone** column. And then select LAN, WAN, VPN, ALL from the **To Zone** column. Click **OK** to display the access rules.

Each view displays a table of defined network access rules. For example, selecting **All Rules** displays all the network access rules for all zones.



## Configuring Access Rules for a Zone

To display the **Access Rules** for a specific zone, select a zone from the **Matrix**, **Drop-down Boxes**, or **All Rules** view.



The access rules are sorted from the most specific at the top, to less specific at the bottom of the table. At the bottom of the table is the **Any** rule. The default access rule is all IP services except those listed in the **Access Rules** page. Access rules can be created to override the behavior of the **Any** rule; for example, the **Any** rule allows users on the LAN to access all Internet services, including NNTP News.



You can change the priority ranking of an access rule by clicking the **Arrows** icon in the Priority column. The Change Priority window is displayed. Enter the new priority number (1-10) in the **Priority** field, and click **OK**.

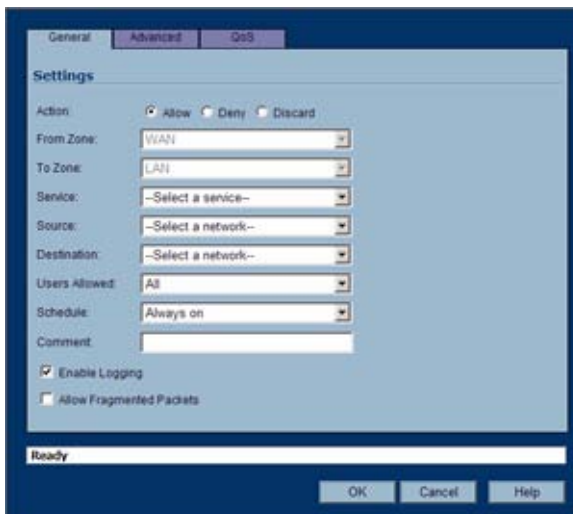
**Tip**

If the **Trashcan** or **Notepad** icons are dimmed (unavailable), the access rule cannot be changed or deleted from the list.

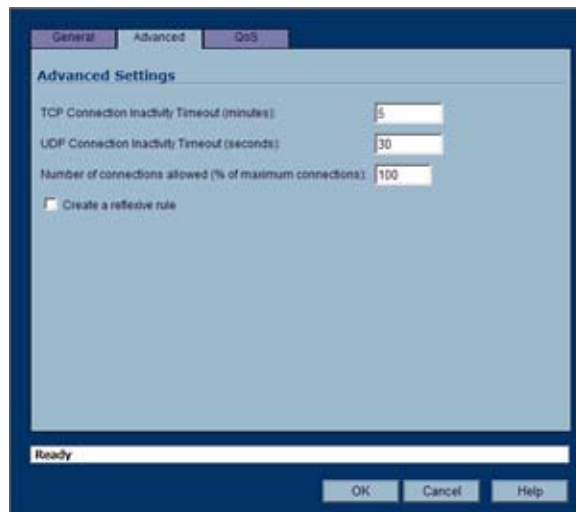
## Adding Access Rules

To add access rules to the SonicWALL security appliance, perform the following steps:

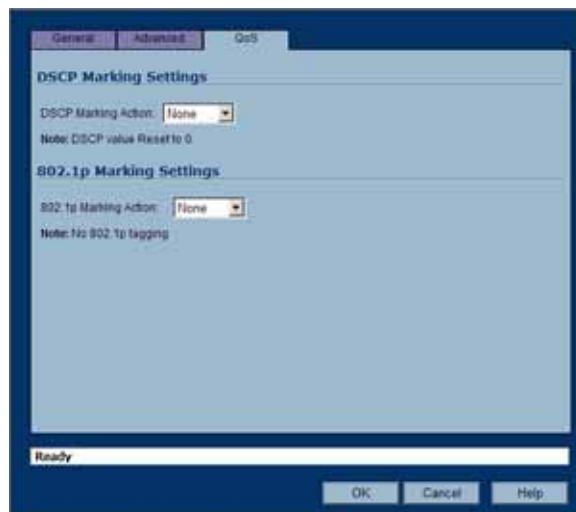
- Step 1** Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.



- Step 2** In the **General** tab, select **Allow | Deny | Discard** from the **Action** list to permit or block IP traffic.
- Step 3** Select the from and to zones from the **From Zone** and **To Zone** menus.
- Step 4** Select the service or group of services affected by the access rule from the **Service** list. The **Default** service encompasses all IP services. If the service is not listed, you must define the service in the **Add Service** window. Select **Create New Service** or **Create New Group** to display the **Add Service** window or **Add Service Group** window.
- Step 5** Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Step 6** If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, type the starting IP addresses of the address range in the **Address Range Begin** field and the ending IP address in the **Address Range End** field. To include all IP addresses, type \* in the **Address Range Begin** field.
- Step 7** Select the destination of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.
- Step 8** From the **Users Allowed** menu, add the user or user group affected by the access rule.
- Step 9** Select a schedule from the **Schedule** menu. The default schedule is **Always on**.
- Step 10** Enter any comments to help identify the access rule in the **Comments** field.
- Step 11** Do not select the **Allow Fragmented Packets** check box. Large IP packets are often divided into fragments before they are routed over the Internet and then reassembled at a destination host. Because hackers exploit IP fragmentation in Denial of Service (DoS) attacks, the SonicWALL security appliance blocks fragmented packets by default. You can override the default configuration to allow fragmented packets over PPTP or IPsec.
- Step 12** Click on the **Advanced** tab.



- Step 13** If you would like for the access rule to timeout after a period of TCP inactivity, set the amount of time, in minutes, in the **TCP Connection Inactivity Timeout (minutes)** field. The default value is **5** minutes.
- Step 14** If you would like for the access rule to timeout after a period of UDP inactivity, set the amount of time, in minutes, in the **UDP Connection Inactivity Timeout (minutes)** field. The default value is **30** minutes.
- Step 15** Specify the number of connections allowed as a percent of maximum number of connections allowed by the SonicWALL security appliance in the **Number of connections allowed (% of maximum connections)** field. Refer to “Connection Limiting Overview” on page 429 for more information on connection limiting.
- Step 16** Select **Create a reflexive rule** if you want to create a matching access rule to this one in the opposite direction--from your destination zone or address object to your source zone or address object.
- Step 17** Click on the **QoS** tab if you want to apply DSCP or 802.1p Quality of Service management to traffic governed by this rule. See “[Firewall > QoS Mapping](#)” section on page 467 for more information on managing QoS marking in access rules.



- Step 18** Under **DSCP Marking Settings** select the **DSCP Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **Preserve** is the default.

- **None:** DSCP values in packets are reset to 0.
- **Preserve:** DSCP values in packets will remain unaltered.
- **Explicit:** Set the DSCP value to the value you select in the **Explicit DSCP Value** field. This is a numeric value between 0 and 63. Some of the standard values are:
  - **0** - Best effort/Default (default)
  - **8** - Class 1
  - **10** - Class 1, Gold (AF11)
  - **12** - Class 1, Silver (AF12)
  - **14** - Class 1, Bronze (AF13)
  - **16** - Class 2
  - **18** - Class 2, Gold (AF21)
  - **20** - Class 2, Silver (AF22)
  - **22** - Class 2, Bronze (AF23)
  - **24** - Class 3
  - **26** - Class 3, Gold (AF31)
  - **27** - Class 3, Silver (AF32)
  - **30** - Class 3, Bronze (AF33)
  - **32** - Class 4
  - **34** - Class 4, Gold (AF41)
  - **36** - Class 4, Silver (AF42)
  - **38** - Class 4, Bronze (AF43)
  - **40** - Express Forwarding
  - **46** - Expedited Forwarding (EF)
  - **48** - Control
  - **56** - Control
- **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [“Firewall > QoS Mapping” section on page 467](#) for instructions on configuring the QoS Mapping. If you select Map, you can select **Allow 802.1p Marking to override DSCP values**.

**Step 19** Under **802.1p Marking Settings** select the **802.1p Marking Action**. You can select **None**, **Preserve**, **Explicit**, or **Map**. **None** is the default.

- **None:** No 802.1p tagging is added to the packets.
- **Preserve:** 802.1p values in packets will remain unaltered.
- **Explicit:** Set the 802.1p value to the value you select in the Explicit 802.1p Value field. This is a numeric value between 0 and 7. The standard values are:
  - **0** - Best effort (default)
  - **1** - Background
  - **2** - Spare
  - **3** - Excellent effort
  - **4** - Controlled load
  - **5** - Video (<100ms latency)

- **6** - Voice (<10ms latency)
  - **7** - Network control
- **Map:** The QoS mapping settings on the **Firewall > QoS Mapping** page will be used. See [“Firewall > QoS Mapping” section on page 467](#) for instructions on configuring the QoS Mapping.

**Step 20** Click **OK** to add the rule.



**Tip**

Although custom access rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from DoS attacks, such as the SYN Flood and Ping of Death attacks.

## Editing an Access Rule

To display the **Edit Rule** window (includes the same settings as the **Add Rule** window), click the **Notepad** icon.

## Deleting an Access Rule

To delete the individual access rule, click on the **Trashcan** icon. To delete all the checkbox selected access rules, click the **Delete** button.

## Enabling and Disabling an Access Rule

To enable or disable an access rule, click the **Enable** checkbox.

## Restoring Access Rules to Default Zone Settings

To remove all end-user configured access rules for a zone, click the **Default** button. This will restore the access rules for the selected zone to the default access rules initially setup on the SonicWALL security appliance.

## Displaying Access Rule Traffic Statistics

Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets

## Connection Limiting Overview

The Connection Limiting feature is intended to offer an additional layer of security and control when coupled with such SonicOS features as SYN Cookies and Intrusion Prevention Services (IPS). Connection limiting provides a means of throttling connections through the SonicWALL using Access Rules as a classifier, and declaring the maximum percentage of the total available connection cache that can be allocated to that class of traffic.

Coupled with IPS, this can be used to mitigate the spread of a certain class of malware as exemplified by Sasser, Blaster, and Nimda. These worms propagate by initiating connections to random addresses at atypically high rates. For example, each host infected with Nimda attempted 300 to 400 connections per second, Blaster sent 850 packets per second, and Sasser was capable of 5,120 attempts per second. Typical, non-malicious network traffic generally does not establish anywhere near these numbers, particularly when it is Trusted ->Untrusted traffic (i.e. LAN->WAN). Malicious activity of this sort can consume all available connection-cache resources in a matter of seconds, particularly on smaller appliances.

The following table delineates the connection-cache size of currently available SonicWALL devices running SonicOS Enhanced (numbers are subject to change):

SonicWALL Security Appliance	Connection Cache Maximum
PRO 4060	524,288
PRO 5060	750,000

In addition to mitigating the propagation of worms and viruses, Connection limiting can be used to alleviate other types of connection-cache resource consumption issues, such as those posed by uncompromised internal hosts running peer-to-peer software (assuming IPS is configured to allow these services), or internal or external hosts using packet generators or scanning tools.

Finally, connection limiting can be used to protect publicly available servers (e.g. web-servers) by limiting the number of legitimate inbound connections permitted to the server (i.e. to protect the server against the Slashdot-effect). This is different from SYN flood protection which attempts to detect and prevent partially-open or spoofed TCP connection. This will be most applicable for Untrusted traffic, but it can be applied to any Zone traffic as needed.

Connection limiting is applied by defining a percentage of the total maximum allowable connections that may be allocated to a particular type of traffic. The above figures show the default LAN ->WAN setting, where all available resources may be allocated to LAN->WAN (any source, any destination, any service) traffic.

More specific rules can be constructed; for example, to limit the percentage of connections that can be consumed by a certain type of traffic (e.g. FTP traffic to any destination on the WAN), or to prioritize important traffic (e.g. HTTPS traffic to a critical server) by allowing 100% to that class of traffic, and limiting general traffic to a smaller percentage (minimum allowable value is 1%).

**Note**

It is not possible to use IPS signatures as a connection limiting classifier; only Access Rules (i.e. Address Objects and Service Objects) are permissible.

## Access Rule Configuration Examples

This section provides configuration examples on adding network access rules:

- [“Enabling Ping” section on page 431](#)
- [“Blocking LAN Access for Specific Services” section on page 431](#)
- [“Enabling Bandwidth Management on an Access Rule” section on page 431](#)

## Enabling Ping

This section provides a configuration example for an access rule to allow devices on the DMZ to send ping requests and receive ping responses from devices on the LAN. By default your SonicWALL security appliance does not allow traffic initiated from the DMZ to reach the LAN. Once you have placed one of your interfaces into the DMZ zone, then from the **Firewall > Access Rules** window, perform the following steps to configure an access rule that allow devices in the DMZ to send ping requests and receive ping responses from devices in the LAN.

- 
- Step 1** Click **Add** to launch the **Add Rule** window.
  - Step 2** Select the **Allow** radio button.
  - Step 3** From the **Service** menu, select **Ping**.
  - Step 4** From the **Source** menu, select **DMZ Subnets**.
  - Step 5** From the **Destination** menu, select **LAN Subnets**.
  - Step 6** Click **OK**.

## Blocking LAN Access for Specific Services

This section provides a configuration example for an access rule blocking LAN access to NNTP servers on the Internet during business hours.

Perform the following steps to configure an access rule blocking LAN access to NNTP servers based on a schedule:

- 
- Step 1** Click **Add** to launch the **Add** window.
  - Step 2** Select **Deny** from the **Action** settings.
  - Step 3** Select **NNTP** from the **Service** menu. If the service is not listed in the list, you must add it in the **Add Service** window.
  - Step 4** Select **Any** from the **Source** menu.
  - Step 5** Select **WAN** from the **Destination** menu.
  - Step 6** Select the schedule from the **Schedule** menu.
  - Step 7** Enter any comments in the **Comment** field.
  - Step 8** Click **OK**.

## Enabling Bandwidth Management on an Access Rule

Bandwidth management can be applied on both ingress and egress traffic using access rules. Access rules displaying the Funnel icon are configured for bandwidth management.



### Tip

**Tip:** Do not configure bandwidth management on multiple interfaces on a zone, where the configured guaranteed bandwidth for the zone is greater than the available bandwidth for the bound interface.

For more information on Bandwidth Management see “Bandwidth Management” on page 479.





# CHAPTER 40

## Configuring Advanced Access Rule Settings

### Firewall > Advanced

To configure advanced access rule options, select **Firewall > Advanced** under Firewall. The **Advanced Rule Options** page is displayed.



The **Advanced Rule Options** includes the following firewall configuration option groups:

- Detection Prevention
- Dynamic Ports
- Source Routed Packets
- Connections
- Access Rule Service Options
- IP and UDP Checksum Enforcement

- UDP

## Detection Prevention

- **Enable Stealth Mode** - By default, the security appliance responds to incoming connection requests as either “blocked” or “open.” If you enable Stealth Mode, your security appliance does not respond to *blocked inbound connection requests*. Stealth Mode makes your security appliance essentially invisible to hackers.
- **Randomize IP ID** - Select Randomize IP ID to prevent hackers using various detection tools from detecting the presence of a security appliance. IP packets are given random IP IDs, which makes it more difficult for hackers to “fingerprint” the security appliance.
- **Decrement IP TTL for forwarded traffic** - Time-to-live (TTL) is a value in an IP packet that tells a network router whether or not the packet has been in the network too long and should be discarded. Select this option to decrease the TTL value for packets that have been forwarded and therefore have already been in the network for some time.
- **Never generate ICMP Time-Exceeded packets** - The SonicWALL appliance generates Time-Exceeded packets to report when it has dropped a packet because its TTL value has decreased to zero. Select this option if you don't want the SonicWALL appliance to generate these reporting packets.

## Dynamic Ports

- **Enable support for Oracle (SQLNet)** - Select if you have Oracle applications on your network.
- **Enable support for Windows Messenger** - Select this option to support special SIP messaging used in Windows Messenger on the Windows XP.
- **Enable RTSP Transformations** - Select this option to support on-demand delivery of real-time data, such as audio and video. RTSP (Real Time Streaming Protocol) is an application-level protocol for control over delivery of data with real-time properties.

## Source Routed Packets

**Drop Source Routed Packets** is selected by default. Clear the check box if you are testing traffic between two specific hosts and you are using source routing.

## Connections

Check **Disable Anti-Spyware, Gateway AV and IPS Engine (increases maximum SPI connections)** if you want to enable more connections at the expense of the Gateway Anti-Virus and Intrusion Prevention services.

## Access Rule Service Options

**Force inbound and outbound FTP data connections to use default port 20** - The default configuration allows FTP connections from port 20 but remaps outbound traffic to a port such as 1024. If the check box is selected, any FTP data connection through the security appliance must come from port 20 or the connection is dropped. The event is then logged as a log event on the security appliance.

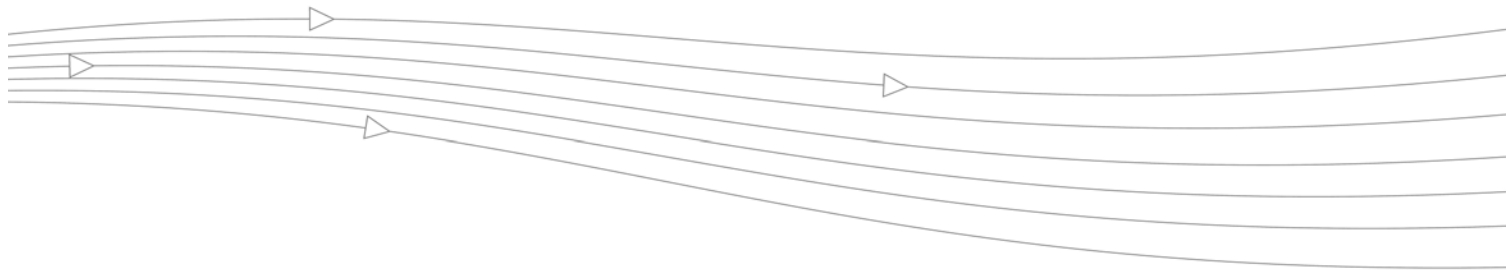
## IP and UDP Checksum Enforcement

- **Enable IP header checksum enforcement** - Select this to enforce IP header checksums.
- **Enable UDP checksum enforcement** - Select this to enforce IP header checksums.

## UDP

Enter the number of seconds of idle time you want to allow before UDP connections time out in the **Default UDP Connection Timeout (seconds)** field. This value is overridden by the UDP Connection timeout you set for individual rules.





# CHAPTER 41

## Configuring TCP Settings

---

### Firewall > TCP Settings

The TCP Settings lets you view statistics on TCP Traffic through the security appliance and manage TCP traffic settings. The page is divided into three sections

- TCP Traffic Statistics
- TCP Settings
- SYN/RST/FIN Flood Protection

### TCP Traffic Statistics

The TCP Traffic Statistics table provides statistics on the following:

- **Connections Opened** – Incremented when a TCP connection initiator sends a SYN, or a TCP connection responder receives a SYN.
- **Connections Closed** – Incremented when a TCP connection is closed when both the initiator and the responder have sent a FIN and received an ACK.
- **Connections Refused** – Incremented when a RST is encountered, and the responder is in a SYN\_RCVD state.
- **Connections Aborted** – Incremented when a RST is encountered, and the responder is in some state other than SYN\_RCVD.
- **Total TCP Packets** – Incremented with every processed TCP packet.
- **Validated Packets Passed** – Incremented under the following conditions:
  - When a TCP packet passes checksum validation (while TCP checksum validation is enabled).
  - When a valid SYN packet is encountered (while SYN Flood protection is enabled).
  - When a SYN Cookie is successfully validated on a packet with the ACK flag set (while SYN Flood protection is enabled).
- **Corrupted Packets Dropped** - Incremented under the following conditions:
  - When TCP checksum fails validation (while TCP checksum validation is enabled).

- When the TCP SACK Permitted (Selective Acknowledgement, see RFC1072) option is encountered, but the calculated option length is incorrect.
- When the TCP MSS (Maximum Segment Size) option is encountered, but the calculated option length is incorrect.
- When the TCP SACK option data is calculated to be either less than the minimum of 6 bytes, or modulo incongruent to the block size of 4 bytes.
- When the TCP option length is determined to be invalid.
- When the TCP header length is calculated to be less than the minimum of 20 bytes.
- When the TCP header length is calculated to be greater than the packet's data length.
- **Invalid Flag Packets Dropped** - Incremented under the following conditions:
  - When a non-SYN packet is received that cannot be located in the connection-cache (while SYN Flood protection is disabled).
  - When a packet with flags other than SYN, RST+ACK or SYN+ACK is received during session establishment (while SYN Flood protection is enabled).
    - TCP XMAS Scan will be logged if the packet has FIN, URG, and PSH flags set.
    - TCP FIN Scan will be logged if the packet has the FIN flag set.
    - TCP Null Scan will be logged if the packet has no flags set.
  - When a new TCP connection initiation is attempted with something other than just the SYN flag set.
  - When a packet with the SYN flag set is received within an established TCP session.
  - When a packet without the ACK flag set is received within an established TCP session.
- **Invalid Sequence Packets Dropped** – Incremented under the following conditions:
  - When a packet within an established connection is received where the sequence number is less than the connection's oldest unacknowledged sequence.
  - When a packet within an established connection is received where the sequence number is greater than the connection's oldest unacknowledged sequence + the connection's last advertised window size.
- **Invalid Acknowledgement Packets Dropped** - Incremented under the following conditions:
  - When a packet is received with the ACK flag set, and with neither the RST or SYN flags set, but the SYN Cookie is determined to be invalid (while SYN Flood protection is enabled).
  - When a packet's ACK value (adjusted by the sequence number randomization offset) is less than the connection's oldest unacknowledged sequence number.
  - When a packet's ACK value (adjusted by the sequence number randomization offset) is greater than the connection's next expected sequence number.

## TCP Settings



The TCP Settings section allows you to:

- **Enable TCP Stateful Inspection** – Enabling TCP stateful inspection requires that all TCP connections rigidly adhere to the following TCP setup requirements:
  - TCP session establishment involves a three-way handshake between two hosts and consists of the following:
    - Initiator --> SYN --> Responder
    - Initiator <-- SYN/ACK <-- Responder
    - Initiator --> ACK --> Responder
    - (Session established)

After the initial SYN, it is permissible for a Client to send a RST or a SYN, or for the Server to send a SYN-ACK or a RST. Any other kind of TCP flags are generally considered invalid, or potentially malicious. The 'Enable TCP Stateful Inspection' option enforces these guidelines, and drops any traffic that violates them.



**Note**

Some legitimate TCP/IP stack implementations do not abide by these rules, and require that 'Enable TCP Stateful Inspection' be disabled. For the sake of compatibility with these implementations, the 'Enable TCP Stateful Inspection' option is disabled by default, but can be enabled to heighten security, or if there is no concern of potential incompatibilities.

- **Enable TCP Checksum Validation** – If an invalid TCP checksum is calculated, the packet will be dropped.
- **Default TCP Connection Timeout** – The default time assigned to Access Rules for TCP traffic. If a TCP session is active for a period in excess of this setting, the TCP connection will be cleared by the SonicWALL. The default value is 5 minutes, the minimum value is 1 minute, and the maximum value is 999 minutes. Note: Setting excessively long connection time-outs will slow the reclamation of stale resources, and in extreme cases could lead to exhaustion of the connection cache.
- **Maximum Segment Lifetime (seconds)** – Determines the number of seconds that any TCP packet is valid before it expires. This setting is also used to determine the amount of time (calculated as twice the Maximum Segment Lifetime, or 2MSL) that an actively closed TCP connection remains in the TIME\_WAIT state to ensure that the proper FIN / ACK exchange has occurred to cleanly close the TCP connection.
  - Default value: 8 seconds
  - Minimum value: 1 second
  - Maximum value: 60 seconds

## Working with SYN/RST/FIN Flood Protection

SYN/RST/FIN Flood protection helps to protect hosts behind the SonicWALL from Denial of Service (DoS) or Distributed DoS attacks that attempt to consume the host's available resources by creating one of the following attack mechanisms:

- Sending TCP SYN packets, RST packets, or FIN packets with invalid or spoofed IP addresses.
- Creating excessive numbers of half-opened TCP connections.

A SYN Flood attack is considered to be in progress if the number of unanswered SYN/ACK packets sent by the SonicWALL (half-opened TCP connections) exceeds the threshold set in the “Flood rate until attack logged (unanswered SYN/ACK packets per second)” field. The default value for the field is 20, the minimum is 5, and the maximum is 999,999.

## Understanding a TCP Handshake

A typical TCP handshake (simplified) begins with an initiator sending a TCP SYN packet with a 32-bit sequence (SEQ<sub>i</sub>) number. The responder then sends a SYN/ACK packet acknowledging the received sequence by sending an ACK equal to SEQ<sub>i</sub>+1 and a random, 32-bit sequence number (SEQ<sub>r</sub>). The responder also maintains state awaiting an ACK from the initiator. The initiator’s ACK packet should contain the next sequence (SEQ<sub>i</sub>+1) along with an acknowledgment of the sequence it received from the responder (by sending an ACK equal to SEQ<sub>r</sub>+1). The exchange looks as follows:

1. Initiator -> SYN (SEQ<sub>i</sub>=0001234567, ACK<sub>i</sub>=0) -> Responder
2. Initiator <- SYN/ACK (SEQ<sub>r</sub>=3987654321, ACK<sub>r</sub>=0001234568) <- Responder
3. Initiator -> ACK (SEQ<sub>i</sub>=0001234568, ACK<sub>i</sub>=3987654322) -> Responder

Because the responder has to maintain state on all half-opened TCP connections, it is possible for memory depletion to occur if SYNs come in faster than they can be processed or cleared by the responder. A half-opened TCP connection did not transition to an established state through the completion of the three-way handshake. When the SonicWALL is between the initiator and the responder, it effectively becomes the responder, brokering, or *proxying*, the TCP connection to the actual responder (private host) it is protecting.

## SYN Flood Protection Methods

The following sections detail some SYN Flood protection methods.

### SYN Flood Protection Using Stateless Cookies

The method of SYN flood protection employed starting with SonicOS Enhanced uses stateless SYN Cookies, which increase reliability of SYN Flood detection, and also improves overall resource utilization on the SonicWALL. With stateless SYN Cookies, the SonicWALL does not have to maintain state on half-opened connections. Instead, it uses a cryptographic calculation (rather than randomness) to arrive at SEQ<sub>r</sub>.

### Layer-Specific SYN Flood Protection Methods

SonicOS Enhanced provides several protections against SYN Floods generated from two different environments: trusted (internal) or untrusted (external) networks. Attacks from *untrusted* WAN networks usually occur on one or more servers protected by the firewall. Attacks from the *trusted* LAN networks occur as a result of a virus infection inside one or more of the trusted networks, generating attacks on one or more local or remote hosts.

To provide a firewall defense to both attack scenarios, SonicOS Enhanced provides two separate SYN Flood protection mechanisms on two different layers. Each gathers and displays SYN Flood statistics and generates log messages for significant SYN Flood events.

- **SYN Proxy (Layer 3)** – This mechanism shields servers inside the trusted network from WAN-based SYN flood attacks, using a SYN Proxy implementation to verify the WAN clients before forwarding their connection requests to the protected server. You can enable SYN Proxy only on WAN interfaces.



- **SYN Blacklisting (Layer 2)** – This mechanism blocks specific devices from generating or forwarding SYN flood attacks. You can enable SYN Blacklisting on any interface.

## Understanding SYN Watchlists

The internal architecture of both SYN Flood protection mechanisms is based on a single list of Ethernet addresses that are the most active devices sending initial SYN packets to the firewall. This list is called a *SYN watchlist*. Because this list contains Ethernet addresses, the device tracks all SYN traffic based on the address of the device forwarding the SYN packet, without considering the IP source or destination address.

Each watchlist entry contains a value called a *hit count*. The hit count value increments when the device receives the an initial SYN packet from a corresponding device. The hit count decrements when the TCP three-way handshake completes. The hit count for any particular device generally equals the number of half-open connections pending since the last time the device reset the hit count. The device default for resetting a hit count is once a second.

The thresholds for logging, SYN Proxy, and SYN Blacklisting are all compared to the hit count values when determining if a log message or state change is necessary. When a SYN Flood attack occurs, the number of pending half-open connections from the device forwarding the attacking packets increases substantially because of the spoofed connection attempts. When you set the attack thresholds correctly, normal traffic flow produces few attack warnings, but the same thresholds detect and deflect attacks before they result in serious network degradation.

## Working with SYN Flood Protection Features

To configure SYN Flood Protection features, go to the Layer 3 SYN Flood Protection - SYN Proxy portion of the Firewall > TCP Settings window that appears as shown in the following figure.

SYN Flood Protection Mode

SYN Proxy Threshold Region

SYN/RST/FIN Blacklisting

SYN Attack Threshold Region

Note that this region contains four regions:

- SYN Flood Protection Mode
- SYN Attack Threshold
- SYN Proxy Options
- SYN/RST/FIN Blacklisting

Each contains various types of SYN Flood Protection. The following sections describe these features.

## Working with SYN Flood Protection Modes

A SYN Flood Protection mode is the level of protection that you can select to defend against half-opened TCP sessions and high-frequency SYN packet transmissions. This feature enables you to set three different levels of SYN Flood Protection:

**Watch and Report Possible SYN Floods** – This option enables the device to monitor SYN traffic on all interfaces on the device and to log suspected SYN flood activity that exceeds a packet count threshold. The feature does not turn on the SYN Proxy on the device so the device forwards the TCP three-way handshake without modification. This is the least invasive level of SYN Flood protection. Select this option if your network is not in a high risk environment.

**Proxy WAN Client Connections When Attack is Suspected** – This option enables the device to enable the SYN Proxy feature on WAN interfaces when the number of incomplete connection attempts per second surpasses a specified threshold. This method ensures the device continues to process valid traffic during the attack and that performance does not degrade. Proxy mode remains enabled until all WAN SYN flood attacks stop occurring or until the device blacklists all of them using the SYN Blacklisting feature. This is the intermediate level of SYN Flood protection. Select this option if your network experiences SYN Flood attacks from internal or external sources.

**Always Proxy WAN Client Connections** – This option sets the device to always use SYN Proxy. This method blocks all spoofed SYN packets from passing through the device. Note that this is an extreme security measure and directs the device to respond to port scans on all TCP ports because the SYN Proxy feature forces the device to respond to all TCP SYN connection attempts. This can degrade performance and can generate a false positive. Select this option only if your network is in a high risk environment.

## Working with SYN Attack Threshold

The SYN Attack Threshold region of the SYN Flood Protection region, provides limits for SYN Flood activity before the device drops packets. The device gathers statistics on WAN TCP connections, keeping track of the maximum and average maximum and incomplete WAN connections per second. Out of these statistics, the device suggests a value for the SYN flood threshold.

Note the two options in the section:

**Use the 300 Value Calculated from Gathered Statistics** – Sets the threshold for the number of incomplete connection attempts per second before the device drops packets at the default value of 300.

**Attack Threshold (Incomplete Connection Attempts/Second)** – Enables you to set the threshold for the number of incomplete connection attempts per second before the device drops packets at any value between 5 and 999,999.

## Working with SYN Proxy Options

When the device applies a SYN Proxy to a TCP connection, it responds to the initial SYN packet with a manufactured SYN/ACK reply, waiting for the ACK in response before forwarding the connection request to the server. Devices attacking with SYN Flood packets do not respond to the SYN/ACK reply. The firewall identifies them by their lack of this type of response and blocks their spoofed connection attempts. SYN Proxy forces the firewall to manufacture a SYN/ACK response without knowing how the server will respond to the TCP options normally provided on SYN/ACK packets.

To provide more control over the options sent to WAN clients when in SYN Proxy mode, you can configure the following two objects:

**SACK (Selective Acknowledgment)** – This parameter controls whether or not Selective ACK is enabled. With SACK enabled, a packet or series of packets can be dropped, and the received informs the sender which data has been received and where holes may exist in the data.

**MSS (Minimum Segment Size)** – This sets the threshold for the size of TCP segments, preventing a segment that is too large to be sent to the targeted server. For example, if the server is an IPsec gateway, it may need to limit the MSS it received to provide space for IPsec headers when tunneling traffic. The firewall cannot predict the MSS value sent to the server when it responds to the SYN manufactured packet during the proxy sequence. Being able to control the size of a segment, enables you to control the manufactured MSS value sent to WAN clients.

The SYN Proxy Threshold region contains the following options:

**All LAN/DMZ servers support the TCP SACK option** – This checkbox enables Selective ACK where a packet can be dropped and the receiving device indicates which packets it received. Enable this checkbox only when you know that all servers covered by the firewall accessed from the WAN support the SACK option.

**Limit MSS sent to WAN clients (when connections are proxied)** – Enables you to enter the maximum Minimum Segment Size value. If you specify an override value for the default of 1460, this indicates that a segment of that size or smaller will be sent to the client in the SYN/ACK cookie. Setting this value too low can decrease performance when the SYN Proxy is always enabled. Setting this value too high can break connections if the server responds with a smaller MSS value.

**Maximum TCP MSS sent to WAN clients.** The value of the MSS. The default is 1460.



**Note**

When using Proxy WAN client connections, remember to set these options conservatively since they only affect connections when a SYN Flood takes place. This ensures that legitimate connections can proceed during an attack.

## Working with SYN/RST/FIN Blacklisting

The SYN/RST/FIN Blacklisting feature is a list that contains devices that exceeded the SYN, RST, and FIN Blacklist attack threshold. The firewall device drops packets sent from blacklisted devices early in the packet evaluation process, enabling the firewall to handle greater amounts of these packets, providing a defense against attacks originating on local networks while also providing second-tier protection for WAN networks.

Devices cannot occur on the SYN/RST/FIN Blacklist and watchlist simultaneously. With blacklisting enabled, the firewall removes devices exceeding the blacklist threshold from the watchlist and places them on the blacklist. Conversely, when the firewall removes a device from the blacklist, it places it back on the watchlist. Any device whose MAC address has been placed on the blacklist will be removed from it approximately three seconds after the flood emanating from that device has ended.

The SYN/RST/FIN Blacklisting region contains the following options:

**Threshold for SYN/RST/FIN flood blacklisting (SYNs / Sec)** – The maximum number of SYN, RST, and FIN packets allowed per second. The default is 1,000. This value should be larger than the SYN Proxy threshold value because blacklisting attempts to thwart more vigorous local attacks or severe attacks from a WAN network.

**Enable SYN/RST/FIN flood blacklisting on all interfaces** – This checkbox enables the blacklisting feature on all interfaces on the firewall.

**Never blacklist WAN machines** – This checkbox ensures that systems on the WAN are never added to the SYN Blacklist. This option is recommended as leaving it unchecked may interrupt traffic to and from the firewall’s WAN ports.

**Always allow SonicWALL management traffic** – This checkbox causes IP traffic from a blacklisted device targeting the firewall’s WAN IP addresses to not be filtered. This allows management traffic, and routing protocols to maintain connectivity through a blacklisted device.

## SYN, RST, and FIN Flood Statistics

You can view SYN, RST and FIN Flood statistics in the lower half of the TCP Traffic Statistics list as shown in the following figure.

TCP Traffic Statistics	
Connections Opened	320
Connections Closed	314
Connections Refused	2
Connections Aborted	10
Connection Handshake Errors	0
Total TCP Packets	6299
Validated Packets Passed	6298
Malformed Packets Dropped	0
Invalid Flag Packets Dropped	1
Invalid Sequence Packets Dropped	0
Invalid Acknowledgement Packets Dropped	0
Max Incomplete WAN Connections / sec	2
Average Incomplete WAN Connections / sec	0
SYN Floods In Progress	0
RST Floods In Progress	0
FIN Floods In Progress	0
Total SYN, RST or FIN Floods Detected	0
TCP Connection SYN-Proxy State (WAN only)	OFF
Current SYN-Blacklisted Machines	0
Current RST-Blacklisted Machines	0
Current FIN-Blacklisted Machines	0
Total SYN-Blacklisting Events	0
Total RST-Blacklisting Events	0
Total FIN-Blacklisting Events	0
Total SYN Blacklist Packets Rejected	0
Total RST Blacklist Packets Rejected	0
Total FIN Blacklist Packets Rejected	0
Invalid SYN Flood Cookies Received	0

SYN, RST, and FIN Flood Related Statistics (Bottom seventeen)

The following are SYN Flood statistics.

Column	Description
Max Incomplete WAN Connections / sec	The maximum number of pending embryonic half-open connections recorded since the firewall has been up (or since the last time the TCP statistics were cleared).
Average Incomplete WAN Connections / sec	The average number of pending embryonic half-open connections, based on the total number of samples since bootup (or the last TCP statistics reset).
SYN Floods in Progress	The number of individual forwarding devices that are currently exceeding either SYN Flood threshold.
RST Floods in Progress	The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
FIN Floods in Progress	The number of individual forwarding devices that are currently exceeding the SYN/RST/FIN flood blacklisting threshold.
Total SYN, RST, or FIN Floods Detected	The total number of events in which a forwarding device has exceeded the lower of either the SYN attack threshold or the SYN/RST/FIN flood blacklisting threshold.
TCP Connection SYN-Proxy State (WAN only)	Indicates whether or not Proxy-Mode is currently on the WAN interfaces.
Current SYN-Blacklisted Machines	The number of devices currently on the SYN blacklist.
Current RST-Blacklisted Machines	The number of devices currently on the RST blacklist.
Current FIN-Blacklisted Machines	The number of devices currently on the FIN blacklist.
Total SYN-Blacklisting Events	The total number of instances any device has been placed on the SYN blacklist.
Total RST-Blacklisting Events	The total number of instances any device has been placed on the RST blacklist.
Total FIN-Blacklisting Events	The total number of instances any device has been placed on the FIN blacklist.
Total SYN Blacklist Packets Rejected	The total number of packets dropped because of the SYN blacklist.
Total RST Blacklist Packets Rejected	The total number of packets dropped because of the RST blacklist.

Column	Description
Total FIN Blacklist Packets Rejected	The total number of packets dropped because of the FIN blacklist.
Invalid SYN Flood Cookies Received	The total number of invalid SYN flood cookies received.

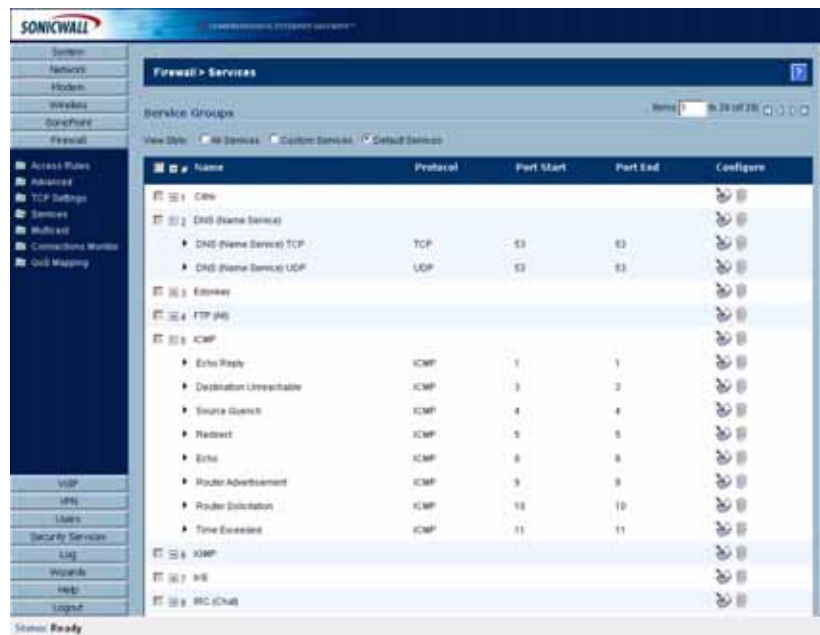
# CHAPTER 42

## Configuring Firewall Services

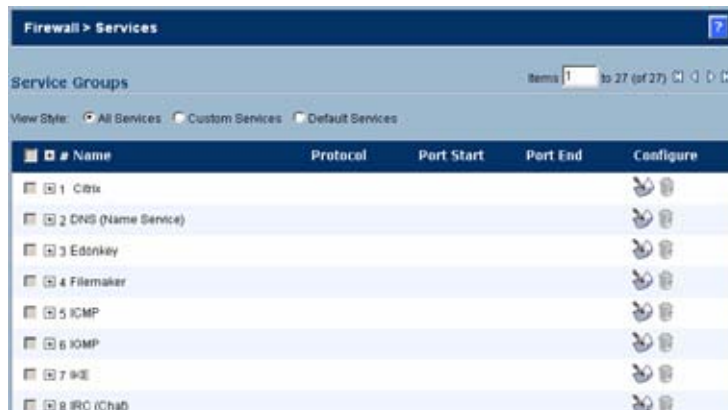
### Firewall > Services

SonicOS Enhanced supports an expanded IP protocol support to allow users to create services and access rules based on these protocols. See “Supported Protocols” on page 449 for a complete listing of support IP protocols.

Services are used by the SonicWALL security appliance to configure network access rules for allowing or denying traffic to the network. The SonicWALL security appliance includes **Default Services**. Default Services are predefined services that are not editable. And you can also create **Custom Services** to configure firewall services to meet your specific business requirements.



Selecting **All Services** from **View Style** displays both **Custom Services** and **Default Services**.



## Default Services Overview

The **Default Services** view displays the SonicWALL security appliance default services in the **Services** table and **Service Groups** table. The Service Groups table displays clusters of multiple default services as a single service object. You cannot delete or edit these predefined services. The **Services** table displays the following attributes of the services:

- **Name**—The name of the service.
- **Protocol**—The protocol of the service.
- **Port Start**—The starting port number for the service.
- **Port End**—The ending port number for the service.
- **Configure**—Displays the unavailable Notepad and Trashcan icon (default services cannot be edited or deleted, you will need to add a new service for the Notepad and Trashcan icons to become available).

Services that apply to common applications are grouped as **Default Service Groups**. These groups cannot be changed or deleted. Clicking on the + to the left of the Default Service Groups entry, displays all the individual Default Services included in the group. For example, the **DNS (Name Service)** entry has two services labelled **DNS (Name Service) TCP** for port 53 and **DNS (Name Service) UDP** for port 53. These multiple entries with the same name are grouped together, and are treated as a single service. Default Services Groups cannot be edited or deleted.

## Custom Services Configuration Task List

The following list provides configuration tasks for Custom Services:

- Adding Custom Services
- Editing Custom Services
- Deleting Custom Services
- Editing Custom Services Groups
- Deleting Custom Services Groups



## Supported Protocols

The following IP protocols are available for custom services:

- **ICMP (1)**—(Internet Control Message Protocol) A TCP/IP protocol used to send error and control messages.
- **IGMP (2)**—(Internet Group Management Protocol) The protocol that governs the management of multicast groups in a TCP/IP network.
- **TCP (6)**—(Transmission Control Protocol) The TCP part of TCP/IP. TCP is a transport protocol in TCP/IP. TCP ensures that a message is sent accurately and in its entirety.
- **UDP (17)**—(User Datagram Protocol) A protocol within the TCP/IP protocol suite that is used in place of TCP when a reliable delivery is not required.
- **GRE (47)**—(Generic Routing Encapsulation) A tunneling protocol used to encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to firewalls or routing devices over an IP internetwork.
- **ESP (50)**—(Encapsulated Security Payload) A method of encapsulating an IP datagram inside of another datagram employed as a flexible method of data transportation by IPsec.
- **AH (51)**—(Authentication Header) A security protocol that provides data authentication and optional anti-relay services. AH is embedded in the data to be protected (a full IP datagram).
- **EIGRP (88)**—(Enhanced Interior Gateway Routing Protocol) Advanced version of IGRP. Provides superior convergence properties and operating efficiency, and combines the advantages of link state protocols with those of distance vector protocols.
- **OSPF (89)**—(Open Shortest Path First) A routing protocol that determines the best path for routing IP traffic over a TCP/IP network based on distance between nodes and several quality parameters. OSPF is an interior gateway protocol (IGP), which is designed to work within an autonomous system. It is also a link state protocol that provides less router to router update traffic than the RIP protocol (distance vector protocol) that it was designed to replace.
- **PIMSM (103)**—(Protocol Independent Multicast Sparse Mode) One of two PIM operational modes (dense and sparse). PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs.
- **L2TP (115)**—(Layer 2 Tunneling Protocol) A protocol that allows a PPP session to run over the Internet. L2TP does not include encryption, but defaults to using IPsec in order to provide virtual private network (VPN) connections from remote users to the corporate LAN.

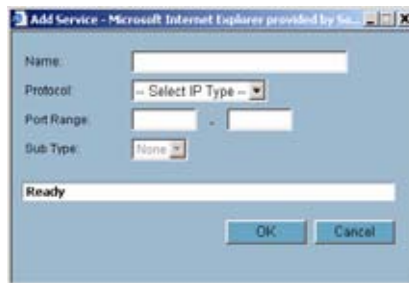
## Adding Custom Services for Predefined Service Types

You can add a custom service for any of the predefined service types:

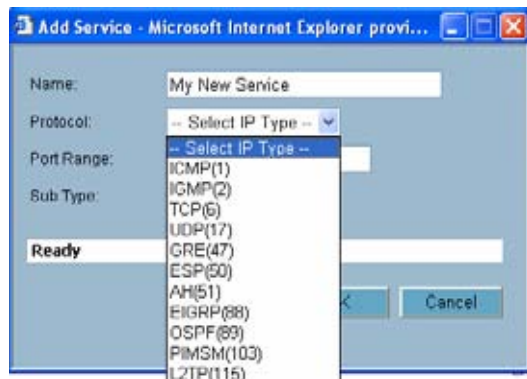
Protocol	IP Number
ICMP	1
TCP	6
UDP	17

GRE	47
IPsec ESP	50
IPsec AH	51
IGMP	2
EIGRP	88
OSPF	89
PIM SM	103
L2T2	115

All custom services you create are listed in the **Custom Services** table. You can group custom services by creating a **Custom Services Group** for easy policy enforcement. If a protocol is not listed in the **Default Services** table, you can add it to the Custom Services table by clicking **Add**.



- Step 1** Enter the name of the service in the **Name** field.
- Step 2** Select the type of IP protocol from the **Protocol** pull-down menu.



- Step 3** Enter the Port Range or IP protocol Sub Type depending on your IP protocol selection:
- For TCP and UDP protocols, specify the Port Range. You will not need to specify a Sub Type.
  - For ICMP, IGMP, OSPF and PIMSM protocols, select from the Sub Type pull-down menu for sub types.
  - For the remaining protocols, you will not need to specify a Port Range or Sub Type.
- Step 4** Click **OK**. The service appears in the **Custom Services** table.

Click the **Enable Logging** checkbox to disable or enable the logging of the service activities.

## Adding Custom IP Type Services

Using only the predefined IP types, if the security appliance encounters traffic of any other IP Protocol type it drops it as *unrecognized*. However, there exists a large and expanding list of other registered IP types, as governed by IANA (Internet Assigned Numbers Authority): <http://www.iana.org/assignments/protocol-numbers>, so while the rigid practice of dropping less-common (unrecognized) IP Type traffic is secure, it was functionally restrictive.

SonicOS Enhanced 3.5 and newer, with its support for Custom IP Type Service Objects, allows an administrator to construct Service Objects representing any IP type, allowing Firewall Access Rules to then be written to recognize and control IPv4 traffic of any type.



### Note

The generic service **Any** will not handle Custom IP Type Service Objects. In other words, simply defining a Custom IP Type Service Object for IP Type 126 will **not** allow IP Type 126 traffic to pass through the default LAN > WAN Allow rule:

Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
1	Any	Any	Any	Allow	All		<input checked="" type="checkbox"/>	

It will be necessary to create an Access Rules specifically containing the Custom IP Type Service Object to provide for its recognition and handling, as illustrated below.

## Example

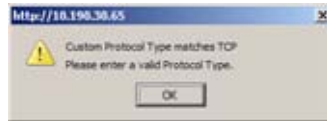
Assume an administrator needed to allow RSVP (Resource Reservation Protocol - IP Type 46) and SRP (Spectralink™ Radio Protocol – IP type 119) from all clients on the WLAN Zone (WLAN Subnets) to a server on the LAN Zone (for example, 10.50.165.26), the administrator would be able to define Custom IP Type Service Objects to handle these two services:

- Step 1** From the **Firewall > Service Objects** page, Services section, select **Add**.
- Step 2** Name the Service Objects accordingly.
- Step 3** Select **Custom IP Type** from the Protocol drop-down list.
- Step 4** Enter the protocol number for the Custom IP Type. *Port ranges are not definable for or applicable to Custom IP types.*



**Note**

Attempts to define a Custom IP Type Service Object for a pre-defined IP type will not be permitted, and will result in an error message.



**Step 5** Click OK



**Step 6** From the **Firewall > Service Objects** page, **Service Group** section, select **Add Group**.

**Step 7** Add a Service Group composed of the Custom IP Types Services.

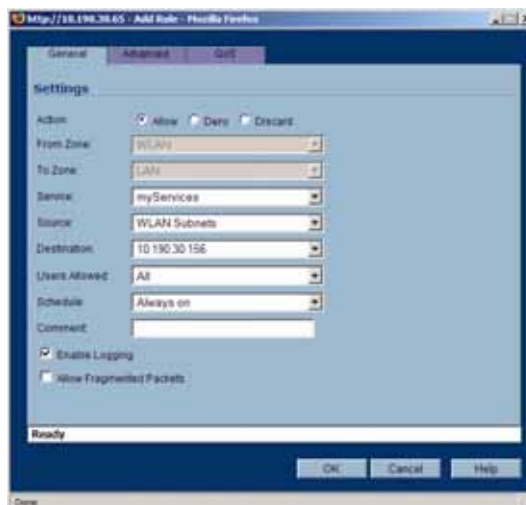


**Step 8** From **Firewall > Access Rules > WLAN > LAN**, select **Add**.

**Step 9** Define an Access Rules allowing **myServices** from **WLAN Subnets** to the **10.50.165.26** Address Object.


**Note**

Select your Zones, Services and Address Objects accordingly. It may be necessary to create an Access Rule for bidirectional traffic; for example, an additional Access Rule from the LAN > WLAN allowing **myServices** from **10.50.165.26** to **WLAN Subnets**.


**Step 10** Click **OK**

IP protocol 46 and 119 traffic will now be recognized, and will be allowed to pass from **WLAN Subnets** to **10.50.165.26**.

## Editing Custom Services

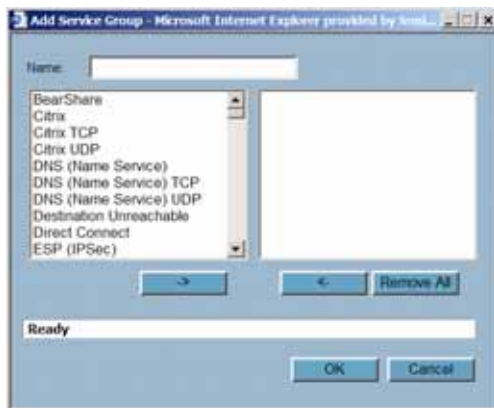
Click the **Edit** icon  under **Configure** to edit the service in the **Edit Service** window, which includes the same configuration settings as the **Add Service** window.

## Deleting Custom Services

Click the **Trashcan** icon  to delete an individual custom service. You can delete all custom services by clicking the **Delete** button.

## Adding a Custom Services Group


You can add custom services and then create groups of services, including default services, to apply the same policies to them. For instance, you can allow SMTP and POP3 traffic only during certain hours or days of the week by adding the two services as a Custom Service Group. To create a **Custom Services Group**, click **Add Group**.




- 
- Step 1** Enter a name for the custom group in the name field.
  - Step 2** Select individual services from the list in the left column. You can also select multiple services by pressing the **Ctrl** key and clicking on the services.
  - Step 3** Click **->** to add the services to the group.
  - Step 4** To remove services from the group, select individual services from the list in right column. You can also select multiple services by pressing the **Ctrl** key on your keyboard and clicking on the services.
  - Step 5** Click **<-** to remove the services.
  - Step 6** When you are finished, click **OK** to add the group to **Custom Services Groups**.

Clicking **+** on the left of a Custom Service Group name, expands the display to show all the individual Custom Services, Default Services, and Custom Services Groups included in the Custom Service Group entry.

## Editing Custom Services Groups

Click the **Edit** icon  under **Configure** to edit the custom service group in the **Edit Service Group** window, which includes the same configuration settings as the **Add Service Group** window.

## Deleting Custom Services Groups

Click the **Trashcan** icon  to delete the individual custom service group entry. You can delete all custom service groups by clicking the Delete button.





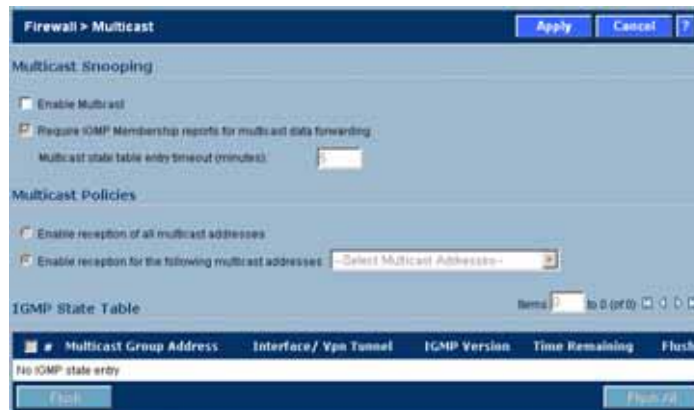
# CHAPTER 43

## Configuring Multicast Settings

### Firewall > Multicast

Multicasting, also called IP multicasting, is a method for sending one Internet Protocol (IP) packet simultaneously to multiple hosts. Multicast is suited to the rapidly growing segment of Internet traffic - multimedia presentations and video conferencing. For example, a single host transmitting an audio or video stream and ten hosts that want to receive this stream. In multicasting, the sending host transmits a single IP packet with a specific multicast address, and the 10 hosts simply need to be configured to listen for packets targeted to that address to receive the transmission. Multicasting is a point-to-multipoint IP communication mechanism that operates in a connectionless mode - hosts receive multicast transmissions by “tuning in” to them, a process similar to tuning in to a radio.

The **Firewall > Multicast** page allows you to manage multicast traffic on the SonicWALL security appliance.



## Multicast Snooping

This section provides configuration tasks for Multicast Snooping.



- **Enable Multicast** - This checkbox is disabled by default. Select this checkbox to support multicast traffic.
- **Require IGMP Membership reports for multicast data forwarding** - This checkbox is enabled by default. Select this checkbox to improve performance by regulating multicast data to be forwarded to only interfaces joined into a multicast group address using IGMP.
- **Multicast state table entry timeout (minutes)** - This field has a default of 5. The value range for this field is 5 to 60 (minutes). Update the default timer value of 5 in the following conditions:
  - You suspect membership queries or reports are being lost on the network.
  - You want to reduce the IGMP traffic on the network and currently have a large number of multicast groups or clients. This is a condition where you do not have a router to route traffic.
  - You want to synchronize the timing with an IGMP router.

## Multicast Policies

This section provides configuration tasks for Multicast Policies.



- **Enable reception of all multicast addresses** - This radio button is not enabled by default. Select this radio button to receive all (class D) multicast addresses. Receiving all multicast addresses may cause your network to experience performance degradation.
- **Enable reception for the following multicast addresses** - This radio button is enabled by default. In the pull-down menu, select **Create a new multicast object** or **Create new multicast group**.

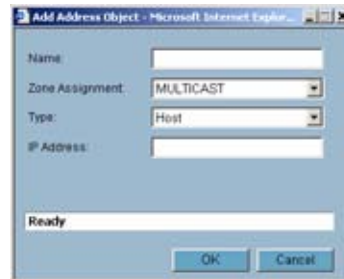


### Note

Only address objects and groups associated with the MULTICAST zone are available to select. Only addresses from 224.0.0.1 to 239.255.255.255 can be bound to the MULTICAST zone.

To create a multicast address object:

- Step 1** In the **Enable reception for the following multicast addresses** list, select **Create new multicast object**.
- Step 2** In the Add Address Object window, configure:



- **Name:** The name of the address object.
- **Zone Assignment:** Select **MULTICAST**.
- **Type:** Select Host, Range, Network, or MAC.
- **IP Address:** If you selected Host or Network, the IP address of the host or network. The IP address must be in the range for multicast, 224.0.0.0 to 239.255.255.255.
- **Netmask:** If you selected Network, the netmask for the network.
- **Starting IP Address** and **Ending IP Address:** If you selected Range, the starting and ending IP address for the address range. The IP addresses must be in the range for multicast, 224.0.0.1 to 239.255.255.255.

## IGMP State Table

This section provides descriptions of the fields in the **IGMP State** table.



- **Multicast Group Address**—Provides the multicast group address the interface is joined to.
- **Interface / VPN Tunnel**—Provides the interface (such as **LAN**) for the VPN policy.
- **IGMP Version**—Provides the IGMP version (such as V2 or V3).
- **Time Remaining**—Provides the amount of time left before the IGMP entry will be flushed. This is calculated by subtracting the “**Multicast state table entry timeout (minutes)**” value, which has the default value of 5 minutes, and the elapsed time since the multicast address was added.
- **Flush** and **Flush All** buttons—To flush a specific entry immediately, check the box to the left of the entry and click **Flush**. Click **Flush All** to immediately flush all entries.

## Enabling Multicast on LAN-Dedicated Interfaces

Perform the following steps to enable multicast support on LAN-dedicated interfaces.

- 
- Step 1** Enable multicast support on your SonicWALL security appliance. In the **Firewall > Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception of all multicast addresses**.
- Step 2** Enable multicast support on LAN interfaces. In the **Network > Interfaces** setting, click on the **'Configure'** icon for the LAN interface. In the **Edit Interface - LAN** page, click on the **Enable Multicast Support** checkbox.

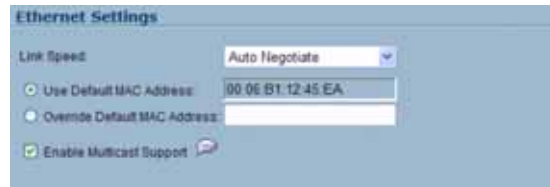
Perform the following steps to enable multicast support for address objects over a VPN tunnel.

- 
- Step 1** Enable multicast support on your SonicWALL security appliance. In the **Firewall > Multicast** setting, click on the **Enable Multicast** checkbox. And in the Multicast Policy section, select the **Enable the reception for the following multicast addresses** and select from the pull-down menu, **Create new multicast address object...**
- Step 2** Create a multicast address object. In the Add Address Object window, enter the following information for your address object:
- Name
  - **Zone Assignment:** <LAN, WAN, DMZ, VPN, MULTICAST, WLAN, or a custom zone>
  - **Type:** <Host, Range, Network>
    - If you select **Host**, you will need to enter an **IP address**.
    - If you select **Range**, you will need to enter a **Starting IP Address** and an **Ending IP Address**.
    - If you select **Network**, you will need to enter a description of the **Network** and a **Netmask**.
    - If you select **MAC**, you will need to enter a **MAC Address**.
- Step 3** Enable multicast support on the VPN policy for your GroupVPN. In the **VPN > Settings** firmware setting, click on the **"Configure"** icon to edit your GroupVPN's VPN policy.
- Step 4** In the **VPN Policy** window, select the **Advanced** tab. At the **Advanced** tab, select the **Enable Multicast** checkbox.

## Enabling Multicast Through a VPN

To enable multicast across the WAN through a VPN, follow:

- Step 1** Enable multicast globally. On the **Firewall > Multicast** page, check the **Enable Multicast** checkbox, and click the **Apply** button for each security appliance.
- Step 2** Enable multicast support on each individual interface that will be participating in the multicast network. On the **Network > Interfaces** page for each interface on all security appliances participating, go to the **Edit Interface: Advanced** tab, and select the **Enable Multicast Support** checkbox.



- Step 3** Enable multicast on the VPN policies between the security appliances. From the **VPN > Settings** page, **Advanced** tab for each policy, select the **Enable Multicast** checkbox.



- Step 4** The resulting Access Rules should look as follows:

#	Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
<b>MULTICAST</b>										
15	LAN > MULTICAST	1	Any	Any	IGMP	Allow	All		✓	
17	LAN > MULTICAST	2	Any	Any	Any	Allow	All		✓	
18	WAN > MULTICAST	1	Any	Any	Membership Query	Allow	All		✓	
19	WAN > MULTICAST	2	Any	Any	IGMP	Deny	All		✓	
20	WAN > MULTICAST	3	Any	Any	Any	Deny	All		✓	
21	DMZ > MULTICAST	1	Any	Any	Membership Query	Allow	All		✓	
22	DMZ > MULTICAST	2	Any	Any	IGMP	Deny	All		✓	
23	DMZ > MULTICAST	3	Any	Any	Any	Allow	All		✓	
24	VPN > MULTICAST	1	Any	Any	IGMP	Allow	All		✓	
25	VPN > MULTICAST	2	Any	Any	Any	Allow	All		✓	
26	WLAN > MULTICAST	1	Any	Any	Membership Query	Allow	All		✓	
27	WLAN > MULTICAST	2	Any	Any	IGMP	Deny	All		✓	
28	WLAN > MULTICAST	3	Any	Any	Any	Deny	All		✓	

**Note**

Notice that the default WLAN/MULTICAST access rule for IGMP traffic is set to 'DENY'. This will need to be changed to 'ALLOW' on all participating appliances to enable multicast, if they have multicast clients on their WLAN zones.

- Step 5** Make sure the tunnels are active between the sites, and start the multicast server application and client applications. As multicast data is sent from the multicast server to the multicast group (224.0.0.0 through 239.255.255.255), the SonicWALL security appliance will query its IGMP state table for that group to determine where to deliver that data. Similarly, when the appliance receives that data at the VPN Zone, it will query its IGMP State Table to determine where it should deliver the data.

The IGMP State Tables (upon updating) should provide information similar to the following:

#	Multicast Group Address	Interface/ Vpn Tunnel	IGMP Version	Time Remaining	Flush
1	224.15.16.17	OPT	V3	3 minute 52 second	
2	224.15.16.17	LAN	V2	3 minute 35 second	

This indicates that there is a multicast client on the **OPT** interface, and across the vpnMcastServer tunnel for the 224.15.16.17 group.

**Note**

By selecting “Enable reception of all multicast addresses”, you might see entries other than those you are expecting to see when viewing your IGMP State Table. These are caused by other multicast applications that might be running on your hosts.

# CHAPTER 44

## Monitoring Active Connections

### Firewall > Connections Monitor

The **Firewall > Connections Monitor** page displays details on all active connections to the security appliance.

The screenshot shows the 'Firewall > Connections Monitor' interface. At the top right, there is a 'Refresh' button and a help icon. Below the title is the 'Active Connections Monitor Settings' section, which includes a table of filter settings:

Filter	Value	Group Filters
Source IP:	<input type="text"/>	<input type="checkbox"/>
Destination IP:	<input type="text"/>	<input type="checkbox"/>
Destination Port:	<input type="text"/>	<input type="checkbox"/>
Protocol:	All Protocols	<input type="checkbox"/>
Src Interface:	All Interfaces	<input type="checkbox"/>
Dst Interface:	All Interfaces	<input type="checkbox"/>

Below the filter settings is the 'Filter Logic' section, which shows the logic: 'Source IP && Destination IP && Destination Port && Protocol && Src Interface && Dst Interface'. There are buttons for 'Apply Filters', 'Reset Filters', and 'Export Results'.

The main section is 'Active Connections Monitor', which displays a table of active connections. The table has columns for '#', 'Source IP', 'Source Port', 'Destination IP', 'Destination Port', 'Protocol', 'Src Interface', 'Dst Interface', 'Tx Bytes', and 'Rx Bytes'. There are two rows of data:

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.118	1936	10.0.93.32	443	TCP	WAN	WAN	1032	2262
2	10.0.202.118	1937	10.0.93.32	443	TCP	WAN	WAN	983	404

## Viewing Connections

The connections are listed in the **Active Connections Monitor** table.

#	Source IP	Source Port	Destination IP	Destination Port	Protocol	Src Interface	Dst Interface	Tx Bytes	Rx Bytes
1	10.0.202.118	2149	10.0.93.32	443	TCP	WAN	WAN	1004	937
2	10.0.202.118	2158	10.0.93.32	443	TCP	WAN	WAN	1005	1393
3	10.0.202.118	2154	10.0.93.32	443	TCP	WAN	WAN	1002	542
4	10.0.202.118	2152	10.0.93.32	443	TCP	WAN	WAN	1049	2485
5	10.0.202.118	2151	10.0.93.32	443	TCP	WAN	WAN	1188	12532
6	10.0.202.118	2159	10.0.93.32	443	TCP	WAN	WAN	1071	404
7	10.0.202.118	2150	10.0.93.32	443	TCP	WAN	WAN	1426	27540
8	10.0.202.118	2157	10.0.93.32	443	TCP	WAN	WAN	1005	1370
9	10.0.202.118	2156	10.0.93.32	443	TCP	WAN	WAN	1005	1411
10	10.0.202.118	2147	10.0.93.32	443	TCP	WAN	WAN	1531	23322
11	10.0.202.118	2148	10.0.93.32	443	TCP	WAN	WAN	1143	9107
12	10.0.202.118	2153	10.0.93.32	443	TCP	WAN	WAN	1739	48015
13	10.0.202.118	2155	10.0.93.32	443	TCP	WAN	WAN	1006	1435

The table lists:

- Source IP
- Source Port
- Destination IP
- Destination Port
- Protocol
- Src Interface
- Dst Interface
- Tx Bytes
- Rx Bytes

Click on a column heading to sort by that column.

## Filtering Connections Viewed

You can filter the results to display only connections matching certain criteria. You can filter by **Source IP**, **Destination IP**, **Destination Port**, **Src Interface**, **Dst Interface**, and **Protocol**. Enter your filter criteria in the **Active Connections Monitor Settings** table.

Filter	Value	Group Filters
Source IP:	192.168.168.1	<input checked="" type="checkbox"/>
Destination IP:	10.16.31.2	<input checked="" type="checkbox"/>
Destination Port:		<input type="checkbox"/>
Protocol:	TCP(6)	<input type="checkbox"/>
Src Interface:	LAN	<input type="checkbox"/>
Dst Interface:	WLAN	<input type="checkbox"/>
<b>Filter Logic:</b>	(Source IP    Destination IP) && Destination Port && Protocol && Src Interface && Dst Interface	
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Results..."/>

The fields you enter values into are combined into a search string with a logical **AND**. For example, if you enter values for **Source IP** and **Destination IP**, the search string will look for connections matching:

*Source IP AND Destination IP*



Check the **Group** box next to any two or more criteria to combine them with a logical **OR**. For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

*(Source IP OR Destination IP) AND Protocol*

Click **Apply Filter** to apply the filter immediately to the **Active Connections** table. Click **Reset** to clear the filter and display the unfiltered results again.

You can export the list of active connections to a file. Click **Export Results**, and select if you want the results exported to a plain text file, or a Comma Separated Value (CSV) file for importing to a spreadsheet, reporting tool, or database. If you are prompted to Open or Save the file, select **Save**. Then enter a filename and path and click **OK**.





## CHAPTER 45

# Managing Quality of Service

---

## Firewall > QoS Mapping

Quality of Service (QoS) refers to a diversity of methods intended to provide predictable network behavior and performance. This sort of predictability is vital to certain types of applications, such as Voice over IP (VoIP), multimedia content, or business-critical applications such as order or credit-card processing. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

This section contains the following subsections:

- [“Classification” section on page 467](#)
- [“Marking” section on page 468](#)
- [“Conditioning” section on page 468](#)

## Classification

Classification is necessary as a first step so that traffic in need of management can be identified. SonicOS Enhanced uses Access Rules as the interface to classification of traffic. This provides fine controls using combinations of Address Object, Service Object, and Schedule Object elements, allowing for classification criteria as general as **all HTTP traffic** and as specific as **SSH traffic from hostA to serverB on Wednesdays at 2:12am**.

SonicOS Enhanced has the ability to recognize, map, modify, and generate the industry-standard external CoS designators, DSCP and 802.1p (refer to the [“802.1p and DSCP QoS” section on page 469](#)).

Once identified, or classified, it can be managed. Management can be performed internally by SonicOS’ BWM, which is perfectly effective as long as the network is a fully contained autonomous system. Once external or intermediate elements are introduced, such as foreign network infrastructures with unknown configurations, or other hosts contending for bandwidth (e.g. the Internet) the ability to offer guarantees and predictability are diminished. In other words, as long as the endpoints of the network and everything in between are within your management, BWM will work exactly as configured. Once external entities are introduced, the precision and efficacy of BWM configurations can begin to degrade.

But all is not lost. Once SonicOS Enhanced classifies the traffic, it can **tag** the traffic to communicate this classification to certain external systems that are capable of abiding by CoS tags; thus they too can participate in providing QoS.

**Note**

Many service providers do not support CoS tags such as 802.1p or DSCP. Also, most network equipment with standard configurations will not be able to recognize 802.1p tags, and could drop tagged traffic.

Although DSCP will not cause compatibility issues, many service providers will simply strip or ignore the DSCP tags, disregarding the code points.

**If you wish to use 802.1p or DSCP marking on your network or your service provider's network, you must first establish that these methods are supported. Verify that your internal network equipment can support CoS priority marking, and that it is correctly configured to do so. Check with your service provider – some offer fee-based support for QoS using these CoS methods.**

## Marking

Once the traffic has been classified, if it is to be handled by QoS capable external systems (e.g. CoS aware switches or routers as might be available on a premium service provider's infrastructure, or on a private WAN), it must be tagged so that the external systems can make use of the classification, and provide the correct handling and Per Hop Behaviors (PHB).

Originally, this was attempted at the IP layer (layer 3) with RFC791's three Precedence bits and RFC1394 ToS (type of service) field, but this was used by a grand total of 17 people throughout history. Its successor, RFC2474 introduced the much more practical and widely used DSCP (Differentiated Services Code Point) which offered up to 64 classifications, as well as user-definable classes. DSCP was further enhanced by RFC2598 (Expedited Forwarding, intended to provide leased-line behaviors) and RFC2697 (Assured Forwarding levels within classes, also known as Gold, Silver, and Bronze levels).

DSCP is a safe marking method for traffic that traverses public networks because there is no risk of incompatibility. At the very worst, a hop along the path might disregard or strip the DSCP tag, but it will rarely mistreat or discard the packet.

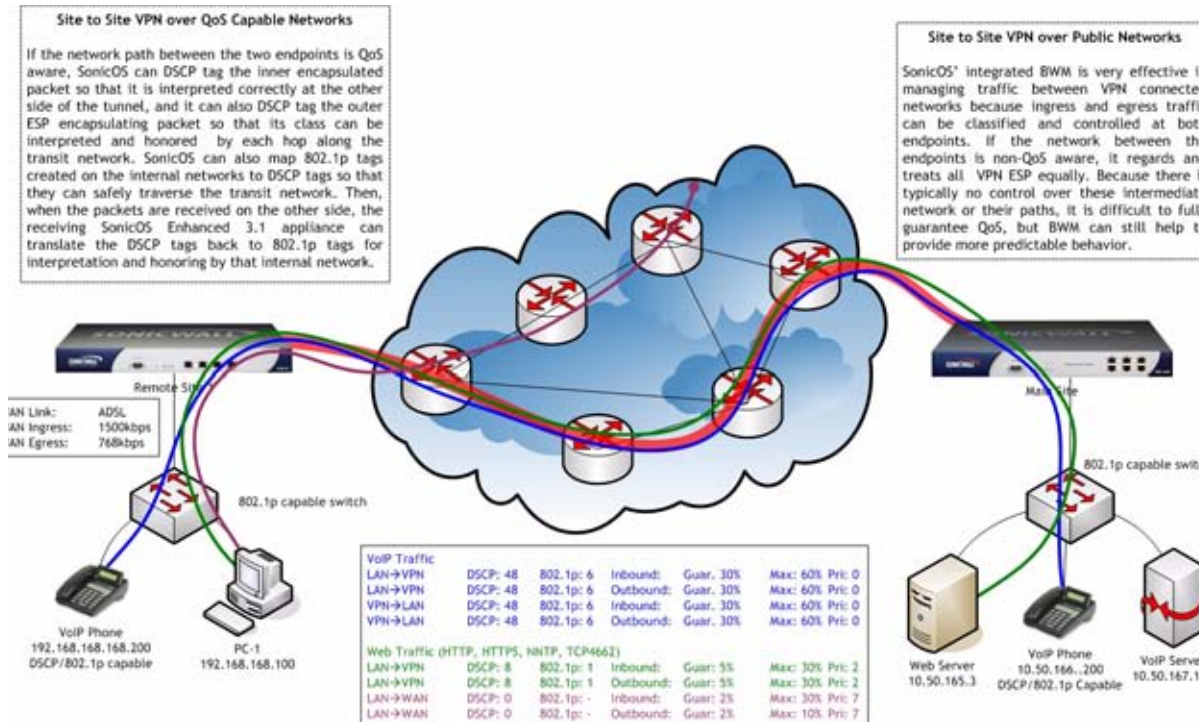
The other prevalent method of CoS marking is IEEE 802.1p. 802.1p occurs at the MAC layer (layer 2) and is closely related to IEEE 802.1Q VLAN marking, sharing the same 16bit field, although it is actually defined in the IEEE 802.1D standard. Unlike DSCP, 802.1p will only work with 802.1p capable equipment, and is not universally interoperable. Additionally, 802.1p, because of its different packet structure, can rarely traverse wide-area networks, even private WANs. Nonetheless, 802.1p is gaining wide support among Voice and Video over IP vendors, so a solution for supporting 802.1p across network boundaries (i.e. WAN links) was introduced in the form of **802.1p to DSCP mapping**.

802.1p to DSCP mapping allows 802.1p tags from one LAN to be mapped to DSCP values by SonicOS Enhanced, allowing the packets to safely traverse WAN links. When the packets arrive on the other side of the WAN or VPN, the receiving SonicOS Enhanced appliance can then map the DSCP tags back to 802.1p tags for use on that LAN. Refer to the ["802.1p and DSCP QoS" section on page 469](#) for more information.

## Conditioning

Finally, the traffic can be conditioned (or managed) using any of the many policing, queuing, and shaping methods available. SonicOS provides internal conditioning capabilities with its Egress and Ingress Bandwidth Management (BWM), detailed in the ["Bandwidth Management"](#)

section on page 479. SonicOS's BWM is a perfectly effective solution for fully autonomous private networks with sufficient bandwidth, but can become somewhat less effective as more unknown external network elements and bandwidth contention are introduced. Refer to the [Example Scenario](#) in the "Example Scenario" section on page 472 for a description of contention issues.



To provide end-to-end QoS, business-class service providers are increasingly offering traffic conditioning services on their IP networks. These services typically depend on the customer premise equipment to classify and tag the traffic, generally using a standard marking method such as DSCP. SonicOS Enhanced has the ability to DSCP mark traffic after classification, as well as the ability to map 802.1p tags to DSCP tags for external network traversal and CoS preservation. For VPN traffic, SonicOS can DSCP mark not only the internal (payload) packets, but the external (encapsulating) packets as well so that QoS capable service providers can offer QoS even on encrypted VPN traffic.

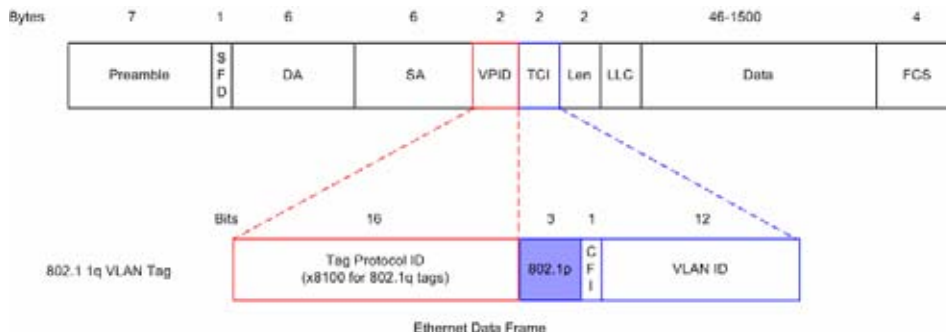
The actual conditioning method employed by service providers varies from one to the next, but it generally involves a class-based queuing method such as Weighted Fair Queuing for prioritizing traffic, as well as a congestion avoidance method, such as tail-drop or Random Early Detection.

## 802.1p and DSCP QoS

The following sections detail the 802.1p standard and DSCP QoS.

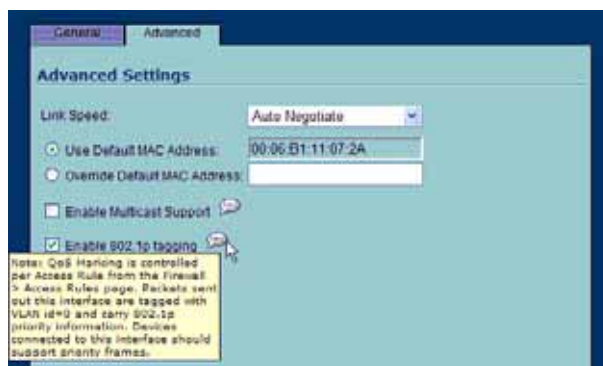
## Enabling 802.1p

SonicOS Enhanced supports layer 2 and layer 3 CoS methods for broad interoperability with external systems participating in QoS enabled environments. The layer 2 method is the IEEE 802.1p standard wherein 3 bits of an additional 16 bits inserted into the header of the Ethernet frame can be used to designate the priority of the frame, as illustrated in the following figure:



- **TPID:** Tag Protocol Identifier begins at byte 12 (after the 6 byte destination and source fields), is 2 bytes long, and has an Ethertype of 0x8100 for tagged traffic.
- **802.1p:** The first three bits of the TCI (Tag Control Information – beginning at byte 14, and spanning 2 bytes) define user priority, giving eight ( $2^3$ ) priority levels. IEEE 802.1p defines the operation for these 3 user priority bits.
- **CFI:** Canonical Format Indicator is a single-bit flag, always set to zero for Ethernet switches. CFI is used for compatibility reasons between Ethernet networks and Token Ring networks. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port.
- **VLAN ID:** VLAN ID (starts at bit 5 of byte 14) is the identification of the VLAN. It has 12 bits and allows for the identification of 4,096 ( $2^{12}$ ) unique VLAN ID's. Of the 4,096 possible IDs, an ID of 0 is used to identify priority frames, and an ID of 4,095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

802.1p support begins by enabling 802.1p marking on the interfaces which you wish to have process 802.1p tags. 802.1p can be enabled on any Ethernet interface on any SonicWALL appliance including the TZ 170 Series, PRO 2040, PRO 3060, PRO 4060, and PRO 5060.



**Note**

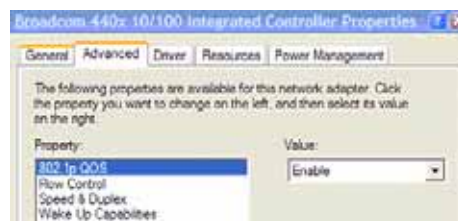
802.1p tagging is not currently supported on the on the PRO 1260.

Although **Enable 802.1p tagging** does not appear as an option on VLAN sub-interfaces on the PRO 4060 and PRO 5060, the 802.1p field is already present within the 802.1q tags of VLAN sub-interfaces. The behavior of the 802.1p field within these tags can be controlled by Access Rules. The default 802.1p Access Rule action of **None** will reset existing 802.1p tags to **0**, unless otherwise configured (see [“Managing QoS Marking” section on page 476](#) for details).

Enabling 802.1p marking will allow the target interface to recognize incoming 802.1p tags generated by 802.1p capable network devices, and will also allow the target interface to generate 802.1p tags, as controlled by Access Rules. Frames that have 802.1p tags inserted by SonicOS will bear VLAN ID 0.

802.1p tags will only be inserted according to Access Rules, so enabling 802.1p marking on an interface will not, at its default setting, disrupt communications with 802.1p-incapable devices.

802.1p requires the specific support by the networking devices with which you wish to use this method of prioritization. Many voice and video over IP devices provide support for 802.1p, but the feature must be enabled. Check your equipment’s documentation for information on 802.1p support if you are unsure. Similarly, many server and host network cards (NICs) have the ability to support 802.1p, but the feature is usually disabled by default. On Win32 operating systems, you can check for and configure 802.1p settings on the **Advanced** tab of the **Properties** page of your network card. If your card supports 802.1p, it will list it as **802.1p QoS**, **802.1p Support**, **QoS Packet Tagging** or something similar:



To process 802.1p tags, the feature must be present and enabled on the network interface. The network interface will then be able to generate packets with 802.1p tags, as governed by QoS capable applications. By default, general network communications will not have tags inserted so as to maintain compatibility with 802.1p-incapable devices.

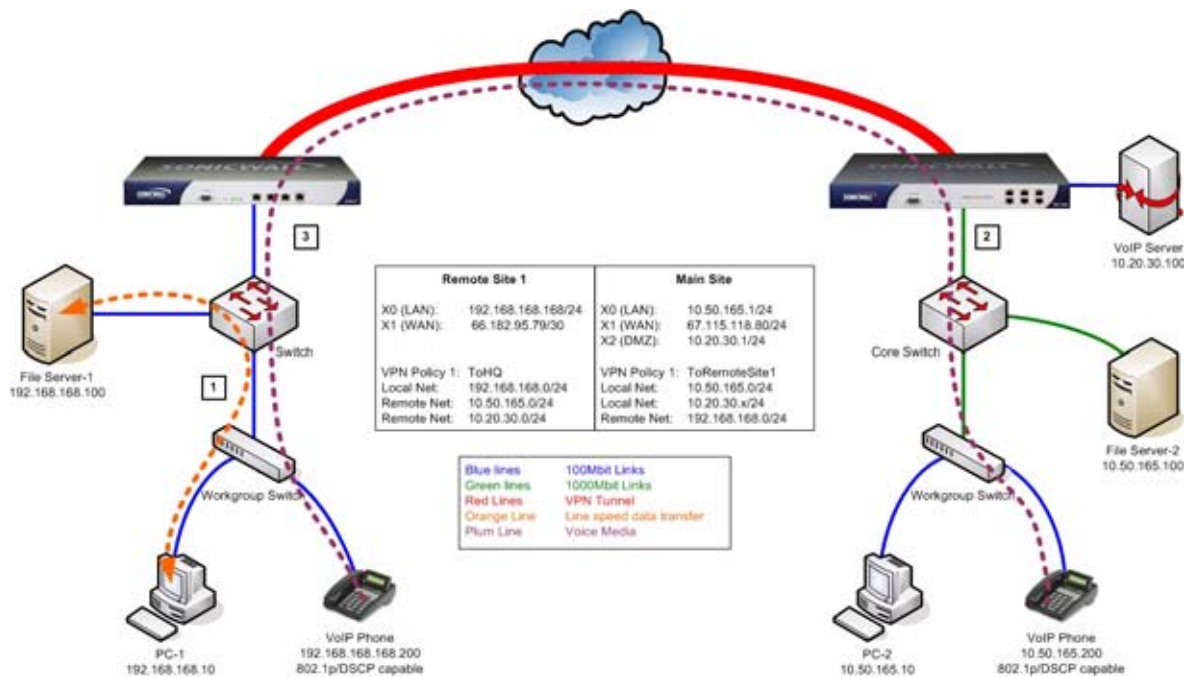
**Note**

If your network interface does not support 802.1p, it will not be able to process 802.1p tagged traffic, and will ignore it. Make certain when defining Access Rules to enable 802.1p marking that the target devices are 802.1p capable.

It should also be noted that when performing a packet capture (for example, with the diagnostic tool Ethereal) on 802.1p capable devices, some 802.1p capable devices will not show the 802.1q header in the packet capture. Conversely, a packet capture performed on an 802.1p-incapable device will almost invariably show the header, but the host will be unable to process the packet.

Before moving on to [“Managing QoS Marking” section on page 476](#), it is important to introduce ‘DSCP Marking’ because of the potential interdependency between the two marking methods, as well as to explain why the interdependency exists.

## Example Scenario



In the scenario above, we have **Remote Site 1** connected to 'Main Site' by an IPsec VPN. The company uses an internal 802.1p/DSCP capable VoIP phone system, with a private VoIP signaling server hosted at the Main Site. The Main Site has a mixed gigabit and Fast-Ethernet infrastructure, while Remote Site 1 is all Fast Ethernet. Both sites employ 802.1p capable switches for prioritization of internal traffic.

1. PC-1 at Remote Site 1 is transferring a 23 terabyte PowerPoint™ presentation to File Server 1, and the 100mbit link between the workgroup switch and the upstream switch is completely saturated.
2. At the Main Site, a caller on the 802.1p/DSCP capable VoIP Phone 10.50.165.200 initiates a call to the person at VoIP phone 192.168.168.200. The calling VoIP phone 802.1p tags the traffic with priority tag 6 (voice), and DSCP tags the traffic with a tag of 48.
  - a. If the link between the Core Switch and the firewall is a VLAN, some switches will include the received 802.1p priority tag, in addition to the DSCP tag, in the packet sent to the firewall; this behavior varies from switch to switch, and is often configurable.
  - b. If the link between the Core Switch and the firewall is not a VLAN, there is no way for the switch to include the 802.1p priority tag. The 802.1p priority is removed, and the packet (including only the DSCP tag) is forwarded to the firewall.

When the firewall sent the packet across the VPN/WAN link, it could include the DSCP tag in the packet, but it is not possible to include the 802.1p tag. This would have the effect of losing all prioritization information for the VoIP traffic, because when the packet arrived at the Remote Site, the switch would have no 802.1p MAC layer information with which to prioritize the traffic. The Remote Site switch would treat the VoIP traffic the same as the lower-priority file transfer because of the link saturation, introducing delay—maybe even dropped packets—to the VoIP flow, resulting in call quality degradation.

So how can critical 802.1p priority information from the Main Site LAN persist across the VPN/WAN link to Remote Site LAN? Through the use of QoS Mapping.



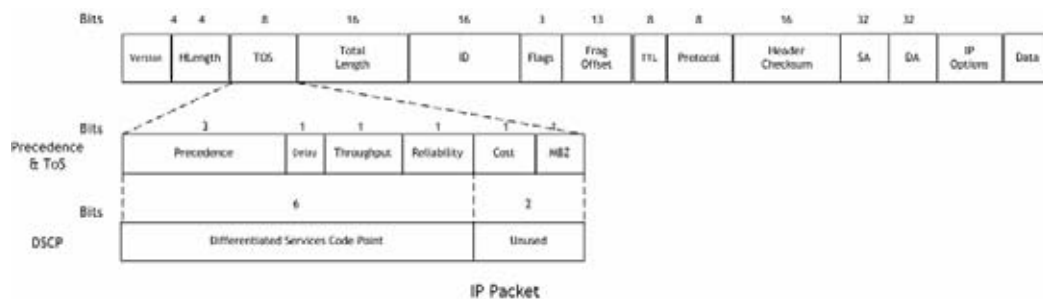
QoS Mapping is a feature which converts layer 2 802.1p tags to layer 3 DSCP tags so that they can safely traverse (in mapped form) 802.1p-incapable links; when the packet arrives for delivery to the next 802.1p-capable segment, QoS Mapping converts from DSCP back to 802.1p tags so that layer 2 QoS can be honored.

In our above scenario, the firewall at the Main Site assigns a DSCP tag (e.g. value **48**) to the VoIP packets, as well as to the encapsulating ESP packets, allowing layer 3 QoS to be applied across the WAN. This assignment can occur either by preserving the existing DSCP tag, or by mapping the value from an 802.1p tag, if present. When the VoIP packets arrive at the other side of the link, the mapping process is reversed by the receiving SonicWALL, mapping the DSCP tag back to an 802.1p tag.

3. The receiving SonicWALL at the Remote Site is configured to map the DSCP tag range 48-55 to 802.1p tag 6. When the packet exits the SonicWALL, it will bear 802.1p tag 6. The Switch will recognize it as voice traffic, and will prioritize it over the file-transfer, guaranteeing QoS even in the event of link saturation.

## DSCP Marking

DSCP (Differentiated Services Code Point) marking uses 6 bits of the 8 bit ToS field in the IP Header to provide up to 64 classes (or code points) for traffic. Since DSCP is a layer 3 marking method, there is no concern about compatibility as there is with 802.1p marking. Devices that do not support DSCP will simply ignore the tags, or at worst, they will reset the tag value to 0.



The above diagram depicts an IP packet, with a close-up on the ToS portion of the header. The ToS bits were originally used for Precedence and ToS (delay, throughput, reliability, and cost) settings, but were later repurposed by RFC2474 for the more versatile DSCP settings.

The following table shows the commonly used code points, as well as their mapping to the legacy Precedence and ToS settings.

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
0	Best effort	0 (Routine – 000)	-
8	Class 1	1 (Priority – 001)	-
10	Class 1, gold (AF11)	1 (Priority – 001)	T
12	Class 1, silver (AF12)	1 (Priority – 001)	D
14	Class 1, bronze (AF13)	1 (Priority – 001)	D, T
16	Class 2	2 (Immediate – 010)	-
18	Class 2, gold (AF21)	2 (Immediate – 010)	T
20	Class 2, silver (AF22)	2 (Immediate – 010)	D
22	Class 2, bronze (AF23)	2 (Immediate – 010)	D, T
24	Class 3	3 (Flash – 011)	-

DSCP	DSCP Description	Legacy IP Precedence	Legacy IP ToS (D, T, R)
26	Class 3, gold (AF31)	3 (Flash - 011)	T
27	Class 3, silver (AF32)	3 (Flash - 011)	D
30	Class 3, bronze (AF33)	3 (Flash - 011)	D, T
32	Class 4	4 (Flash Override - 100)	-
34	Class 4, gold (AF41)	4 (Flash Override - 100)	T
36	Class 4, silver (AF42)	4 (Flash Override - 100)	D
38	Class 4, bronze (AF43)	4 (Flash Override - 100)	D, T
40	Express forwarding	5 (CRITIC/ECP - 101)	-
46	Expedited forwarding (EF)	5 (CRITIC/ECP - 101)	D, T
48	Control	6 (Internet Control - 110)	-
56	Control	7 (Network Control - 111)	-

DSCP marking can be performed on traffic to/from any interface and to/from any zone type, without exception. DSCP marking is controlled by Access Rules, from the QoS tab, and can be used in conjunction with 802.1p marking, as well as with SonicOS' internal bandwidth management.

### DSCP Marking and Mixed VPN Traffic

Among their many security measures and characteristics, IPsec VPNs employ anti-replay mechanisms based upon monotonically incrementing sequence numbers added to the ESP header. Packets with duplicate sequence numbers are dropped, as are packets that do not adhere to sequence criteria. One such criterion governs the handling of out-of-order packets. SonicOS Enhanced provides a replay window of 64 packets, i.e. if an ESP packet for a Security Association (SA) is delayed by more than 64 packets, the packet will be dropped.

This should be considered when using DSCP marking to provide layer 3 QoS to traffic traversing a VPN. If you have a VPN tunnel that is transporting a diversity of traffic, some that is being DSCP tagged high priority (e.g. VoIP), and some that is DSCP tagged low-priority, or untagged/best-effort (e.g. FTP), your service provider will prioritize the handling and delivery of the high-priority ESP packets over the best-effort ESP packets. Under certain traffic conditions, this can result in the best-effort packets being delayed for more than 64 packets, causing them to be dropped by the receiving SonicWALL's anti-replay defenses.

If symptoms of such a scenario emerge (e.g. excessive retransmissions of low-priority traffic), it is recommended that you create a separate VPN policy for the high-priority and low-priority classes of traffic. This is most easily accomplished by placing the high-priority hosts (e.g. the VoIP network) on their own subnet.

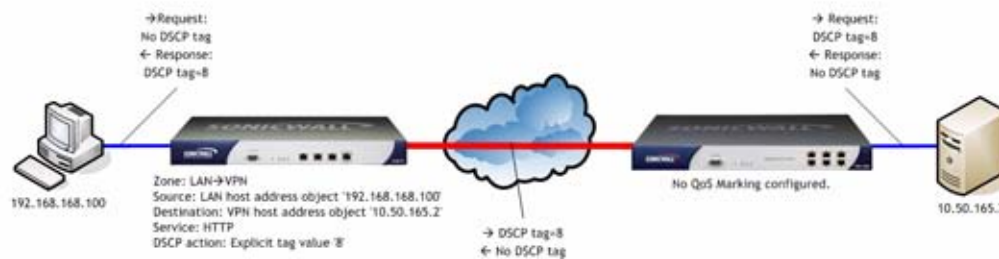
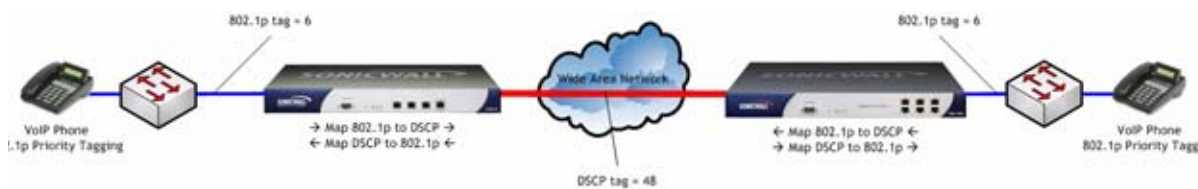


## Configure for 802.1p CoS 4 – Controlled load

If you want to change the inbound mapping of DSCP tag **15** from its default 802.1p mapping of **1** to an 802.1p mapping of **2**, it would have to be done in two steps because mapping ranges cannot overlap. Attempting to assign an overlapping mapping will give the error **DSCP range already exists or overlaps with another range**. First, you will have to remove **15** from its current end-range mapping to 802.1p CoS **1** (changing the end-range mapping of 802.1p CoS **1** to DSCP **14**), then you can assign DSCP **15** to the start-range mapping on 802.1p CoS **2**.

## QoS Mapping

The primary objective of QoS Mapping is to allow 802.1p tags to persist across non-802.1p compliant links (e.g. WAN links) by mapping them to corresponding DSCP tags before sending across the WAN link, and then mapping from DSCP back to 802.1p upon arriving at the other side:



**Note** Mapping will not occur until you assign **Map** as an action of the QoS tab of an Access Rule. The mapping table only defines the correspondence that will be employed by an Access Rule's Map action.

802.1p Class Of Service	To DSCP	From DSCP Range	Configure
0 - Best effort	0 - Best effort/Default	0-7	
1 - Background	8 - Class 1	8-15	
2 - Spare	16 - Class 2	16-23	
3 - Excellent effort	24 - Class 3	24-31	
4 - Controlled load	32 - Class 4	32-39	
5 - Video (~100ms latency)	40 - Express forwarding	40-47	
6 - Voice (~10ms latency)	48 - Control	48-55	
7 - Network control	56 - Control	56-63	

[Reset QoS Settings...](#)

For example, according to the default table, an 802.1p tag with a value of **2** will be outbound mapped to a DSCP value of **16**, while a DSCP tag of **43** will be inbound mapped to an 802.1p value of **5**.

Each of these mappings can be reconfigured. If you wanted to change the outbound mapping of 802.1p tag **4** from its default DSCP value of **32** to a DSCP value of **43**, you can click the **Configure** icon for **4 – Controlled load** and select the new **To DSCP** value from the drop-down box:



802.1p CoS 1 end-range remap



802.1p CoS 2 start-range remap

You can restore the default mappings by clicking the **Reset QoS Settings** button.

### Managing QoS Marking

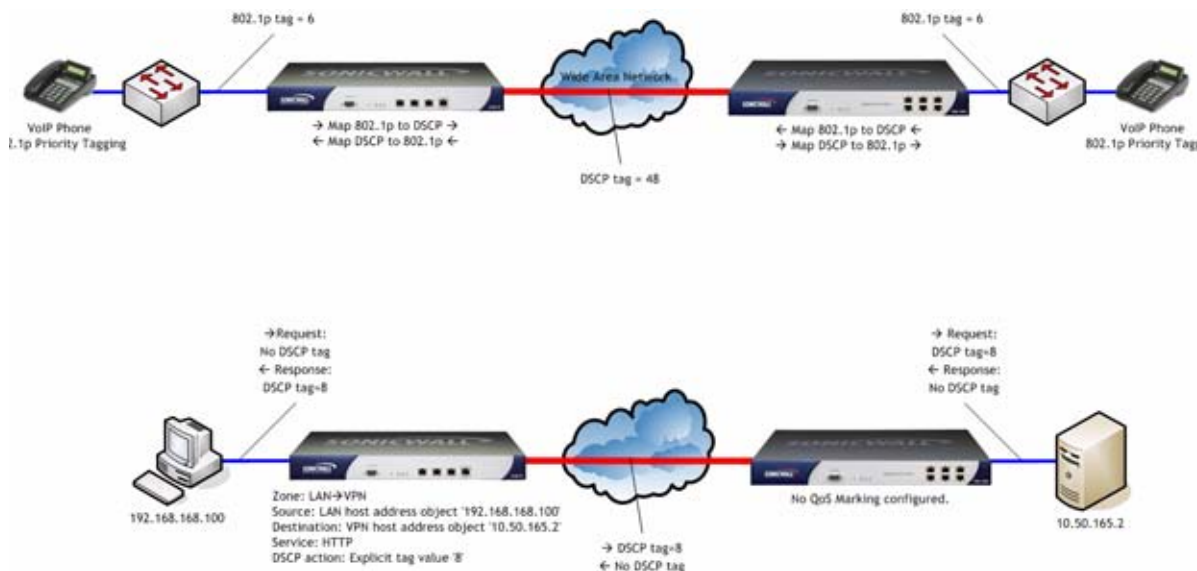
QoS marking is configured from the **QoS** tab of Access Rules under the **Firewall > Access Rules** page of the management interface. Both 802.1p and DSCP marking as managed by SonicOS Enhanced Access Rules provide 4 actions: None, Preserve, Explicit, and Map. The default action for DSCP is **Preserve** and the default action for 802.1p is **None**.

The following table describes the behavior of each action on both methods of marking:

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
None	When packets matching this class of traffic (as defined by the Access Rule) are sent out the egress interface, no 802.1p tag will be added.	The DSCP tag is explicitly set (or reset) to 0.	If the target interface for this class of traffic is a VLAN sub-interface, the 802.1p portion of the 802.1q tag will be explicitly set to 0. If this class of traffic is destined for a VLAN and is using 802.1p for prioritization, a specific Access Rule using the <b>Preserve</b> , <b>Explicit</b> , or <b>Map</b> action should be defined for this class of traffic.
Preserve	Existing 802.1p tag will be preserved.	Existing DSCP tag value will be preserved.	

Action	802.1p (layer 2 CoS)	DSCP (layer 3)	Notes
Explicit	An explicit 802.1p tag value can be assigned (0-7) from a drop-down menu that will be presented.	An explicit DSCP tag value can be assigned (0-63) from a drop-down menu that will be presented.	If either the 802.1p or the DSCP action is set to <b>Explicit</b> while the other is set to <b>Map</b> , the explicit assignment occurs first, and then the other is mapped according to that assignment.
Map	The mapping setting defined in the <b>Firewall &gt; QoS Mapping</b> page will be used to map from a DSCP tag to an 802.1p tag.	The mapping setting defined in the <b>Firewall &gt; QoS Mapping</b> page will be used to map from an 802.1 tag to a DSCP tag. An additional checkbox will be presented to Allow <b>802.1p Marking to override DSCP values</b> . Selecting this checkbox will assert the mapped 802.1p value over any DSCP value that might have been set by the client. This is useful to override clients setting their own DSCP CoS values.	If <b>Map</b> is set as the action on both DSCP and 802.1p, mapping will only occur in one direction: if the packet is from a VLAN and arrives with an 802.1p tag, then DSCP will be mapped to the 802.1p tag; if the packet is destined to a VLAN, then 802.1p will be mapped to the DSCP tag.

For example, refer to the following figure which provides a bi-directional DSCP tag action.



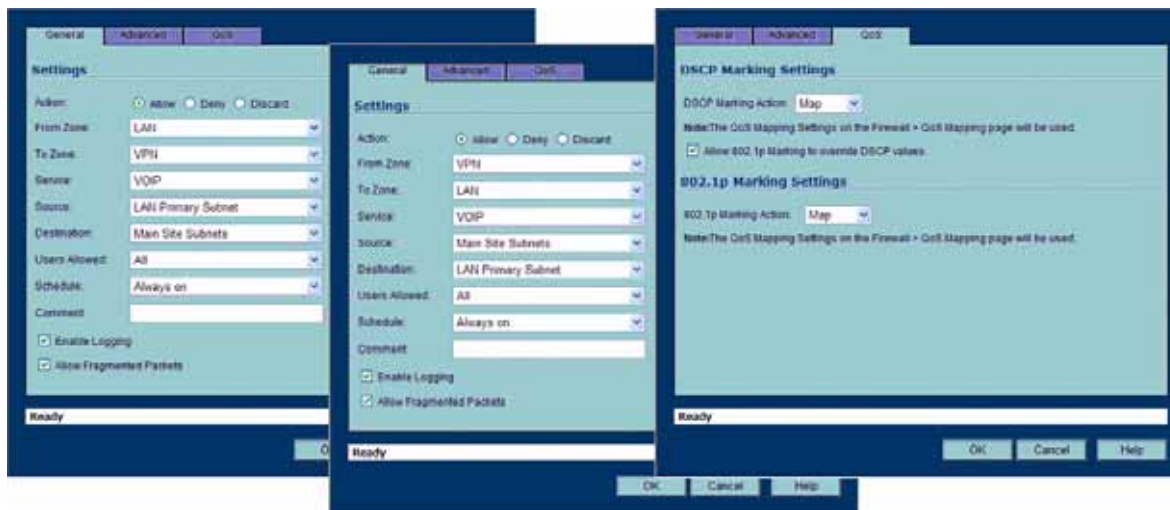
HTTP access from a web-browser on 192.168.168.100 to the web-server on 10.50.165.2 will result in the tagging of the inner (payload) packet and the outer (encapsulating ESP) packets with a DSCP value of 8. When the packets emerge from the other end of the tunnel, and are delivered to 10.50.165.2, they will bear a DSCP tag of 8. When 10.50.165.2 sends response packets back across the tunnel to 192.168.168.100 (beginning with the very first SYN/ACK packet) the Access Rule will tag the response packets delivered to 192.168.168.100 with a DSCP value of 8.

This behavior applies to all four QoS action settings for both DSCP and 802.1p marking.

One practical application for this behavior would be configuring an 802.1p marking rule for traffic destined for the VPN Zone. Although 802.1p tags cannot be sent across the VPN, reply packets coming back across the VPN can be 802.1p tagged on egress from the tunnel. This requires that 802.1p tagging is active of the physical egress interface, and that the [Zone] > VPN Access Rule has an 802.1p marking action other than None.

After ensuring 802.1p compatibility with your relevant network devices, and enabling 802.1p marking on applicable SonicWALL interfaces, you can begin configuring Access Rules to manage 802.1p tags.

Referring to the following figure, the **Remote Site 1** network could have two Access Rules configured as follows:

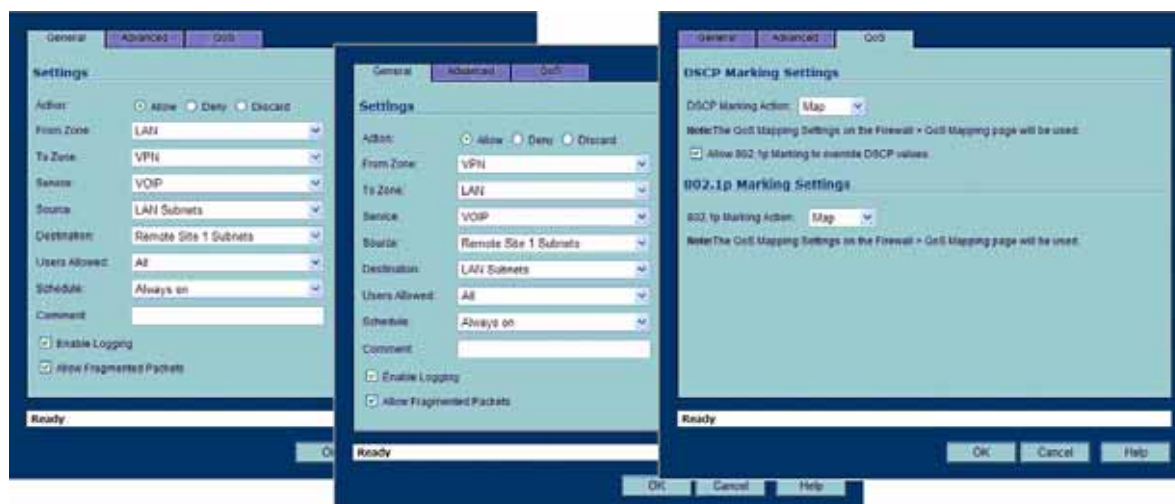


The first Access Rule (governing **LAN>VPN**) would have the following effects:

- **VoIP** traffic (as defined by the Service Group) from **LAN Primary Subnet** destined to be sent across the VPN to **Main Site Subnets** would be evaluated for both DSCP and 802.1p tags.
  - The combination of setting both DSCP and 802.1p marking actions to **Map** is described in the table earlier in the [“Managing QoS Marking”](#) section on page 476.
  - Sent traffic containing only an 802.1p tag (e.g. CoS = 6) would have the VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.
  - Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
  - Sent traffic containing only a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved on both inner and outer packets.
  - Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.
  - Sent traffic containing only both an 802.1p tag (e.g. CoS = 6) and a DSCP tag (e.g. CoS = 63) would give precedence to the 802.1p tag, and would be mapped accordingly. The VPN-bound inner (payload) packet DSCP tagged with a value of 48. The outer (ESP) packet would also be tagged with a value of 48.

Assuming returned traffic has been DSCP tagged (CoS = 48) by the SonicWALL at the Main Site, the return traffic will be 802.1p tagged with CoS = 6 on egress.

To examine the effects of the second Access Rule (VPN>LAN), we'll look at the Access Rules configured at the Main Site:



**VoIP** traffic (as defined by the Service Group) arriving from **Remote Site 1 Subnets** across the VPN destined to **LAN Subnets** on the LAN zone at the Main Site would hit the Access Rule for inbound VoIP calls. Traffic arriving at the VPN zone will not have any 802.1p tags, only DSCP tags.

- Traffic exiting the tunnel containing a DSCP tag (e.g. CoS = 48) would have the DSCP value preserved. Before the packet is delivered to the destination on the LAN, it will also be 802.1p tagged according to the **QoS Mapping** settings (e.g. CoS = 6) by the SonicWALL at the Main Site.
- Assuming returned traffic has been 802.1p tagged (e.g. CoS = 6) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been DSCP tagged (e.g. CoS = 48) by the VoIP phone receiving the call at the Main Site, the return traffic will have the DSCP tag preserved on both the inner and outer packet sent back across the VPN.
- Assuming returned traffic has been both 802.1p tagged (e.g. CoS = 6) and DSCP tagged (e.g. CoS = 14) by the VoIP phone receiving the call at the Main Site, the return traffic will be DSCP tagged according to the conversion map (CoS = 48) on both the inner and outer packet sent back across the VPN.

## Bandwidth Management

SonicOS Enhanced offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) bandwidth management (BWM) interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public Zones (e.g. LAN and DMZ) destined to Untrusted and Encrypted Zones (e.g. WAN and VPN). Inbound BWM can be applied to traffic sourced from Untrusted and Encrypted Zones destined to Trusted and Public Zones.

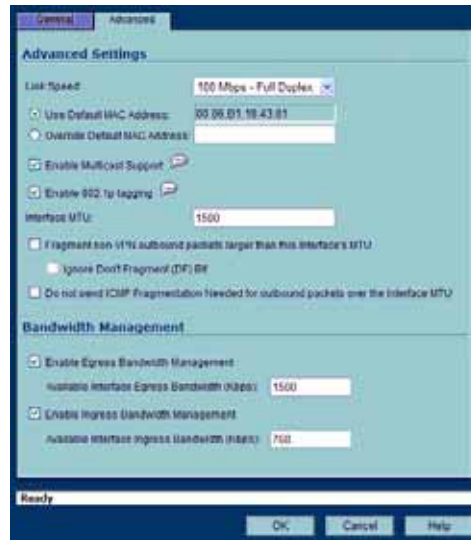


**Note**

Although BWM is a fully integrated QoS system, wherein classification and shaping is performed on the single SonicWALL appliance, effectively eliminating the dependency on external systems and thus obviating the need for marking, it is possible to concurrently

configure **BWM** and **QoS** (i.e. layer 2 and/or layer 3 marking) settings on a single Access Rule. This allows those external systems to benefit from the classification performed on the SonicWALL even after it has already shaped the traffic.

BWM configurations begin by enabling BWM on the relevant WAN interface, and declaring the interface's available bandwidth in Kbps (Kilobits per second). This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:



Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The speed declared should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

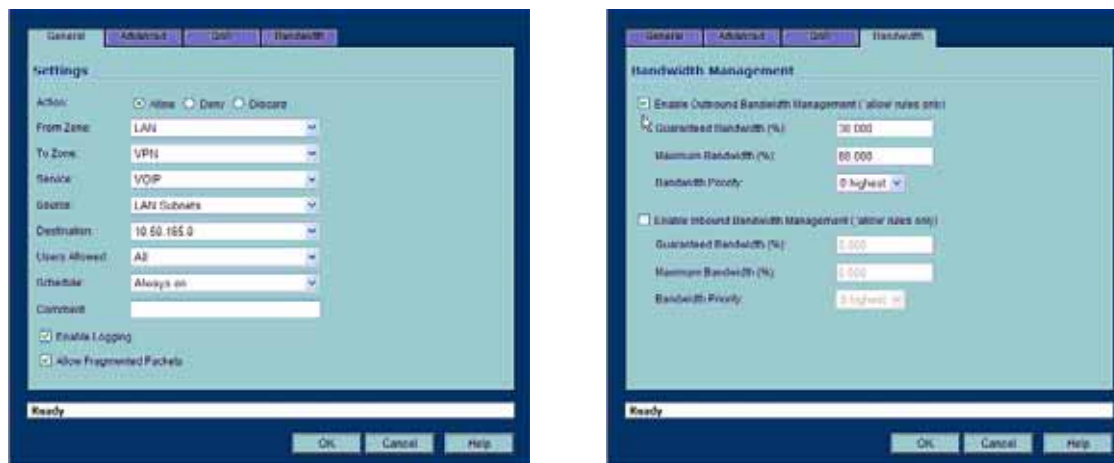


**Note**

Once BWM has been enabled on an interface, and a link speed has been defined, traffic traversing that link will be throttled—both inbound and outbound—to the declared values, even if no Access Rules are configured with BWM settings.



Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Ethernet BWM** tab will appear on Access Rules. The Bandwidth tab will present either **Inbound** settings, **Outbound** settings, or both, depending on what was enabled on the WAN interface:



The configuration on the **General** tab will classify the traffic. In the above example, which assumes no other configured BWM rules, traffic from the LAN (Trusted) Zone's **LAN Subnets** destined to the VPN (Encrypted) Zone's **10.50.165.0** remote subnet, consisting of Service Group **VOIP** will be guaranteed 30% of the declared bandwidth (30% of 1500Kbps = 450Kbps), but it will not be permitted to exceed 80% (80% of 1500Kbps = 1200Kbps), leaving 300Kbps for other traffic.

## Declaration Limits

Bandwidth Management rules each consume memory for packet queuing, so the number of allowed queued packets and rules on SonicOS Enhanced is limited by platform (values are subject to change):

Platform	RAM	Max Queued Packets	Max Outbound BWM Rules	Max Inbound BWM Rules	Total BWM Rules
PRO 4060	256MB	2080	100	100	200
PRO 5060	512MB	6240	100	100	200

Consider the following about bandwidth management:

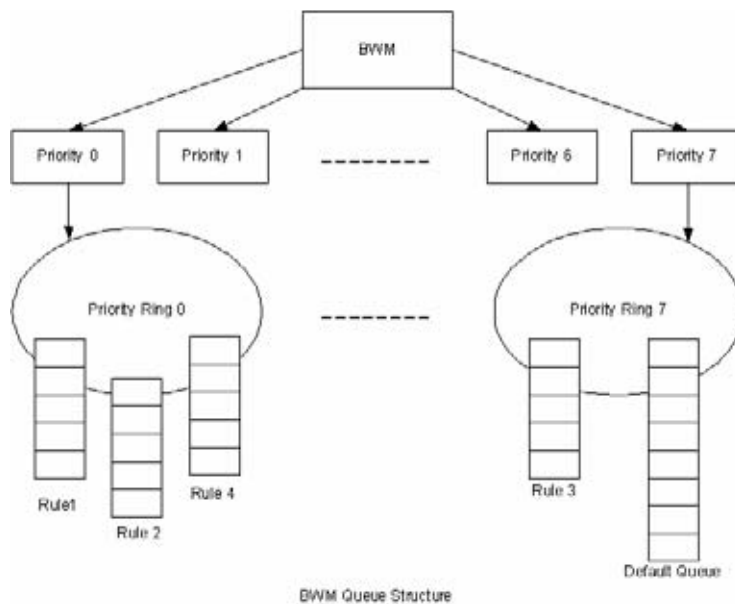
- The grand total of all declared Guaranteed Bandwidth percentages across all BWM rules cannot exceed 100%, since it is not possible to guarantee greater than 100% of the available bandwidth.
- The grand total of all Maximum Bandwidth values must be equal to or greater than the total Guaranteed Bandwidth.
- The grand total of all Maximum Bandwidth values may exceed 100% (e.g. every BWM rule may specify 100% Maximum Bandwidth, if no explicit throttling is required).

## Outbound Bandwidth Management

Bandwidth Management as employed by SonicOS Enhanced is based on an amalgamation of queue management and congestion avoidance techniques, but in empirical practice it most closely resembles Class Base Queuing (CBQ), as defined by Sally Floyd and Van Jacobson in **Link-sharing and Resource Management Models for Packet Networks**, while incorporating elements of RFC2309 **Recommendations on Queue Management and Congestion Avoidance in the Internet** and various credit-based flow control theory. The overarching goals of the SonicOS BWM scheme are:

- **Simplicity** – The processing overhead must be consistently and appreciably less than average packet transmission times.
- **Robustness** – The scheduler must perform well under predictable and unpredictable traffic conditions, and must not introduce undesirable side effects such as traffic bursts or synchronization issues.
- **Fairness** – The sharing of available bandwidth should be commensurate with the defined management scheme, particularly in the presence of poorly behaving or **greedy** traffic.

The available bandwidth on a WAN link is tracked by means of adjusting a link credit (token) pool for each packet sent. Providing that the link hasn't reached a point of saturation, the prioritized queues are deemed eligible for processing.



Like CBQ, SonicOS BWM is based on a class structure, where traffic queues are classified according to Access Rules—for example SSH, Telnet, or HTTP—and then scheduled according to their prescribed priority. Each participating Access Rule is assigned three values: Guaranteed bandwidth, Maximum bandwidth, and Bandwidth priority. Scheduling prioritization is achieved by assignment to one of eight priority rings, starting at 0 (zero) for the highest priority, and descending to 7 (seven) for the lowest priority. The resulting queuing hierarchy can be best thought of as a node tree structure that is always one level deep, where all nodes are leaf nodes, containing no children.

Queue processing utilizes a time division scheme of approximately 1/256th of a second per time-slice. Within a time-slice, evaluation begins with priority 0 queues, and on a packet-by-packet basis transmission eligibility is determined by measuring the packet's length against the queue credit pool. If sufficient credit is available, the packet is transmitted and the queue and link credit pools are decremented accordingly. As long as packets remain in the queue, and as long as Guaranteed link and queue credits are available, packets from that queue will continue

to be processed. When Guaranteed queue credits are depleted, the next queue in that priority ring is processed. The same process is repeated for the remaining priority rings, and upon completing priority ring 7 begins again with priority ring 0.

The scheduling for excess bandwidth is strict priority, with per-packet round-robin within each priority. In other words, if there is excess bandwidth for a given time-slice all the queues within that priority ring would take turns sending packets until the excess was depleted, and then processing would move to the next priority ring.

This credit-based method obviates the need for CBQ's concept of **overlimit**, and addresses one of the largest problems of traditional CBQ, namely, **bursty** behavior (which can easily flood downstream devices and links). This more prudent approach spares SonicOS the wasted CPU cycles that would normally be incurred by the need for re-transmission due to the saturation of downstream devices, as well as avoiding other congestive and degrading behaviors such as TCP slow-start (see Sally Floyd's *Limited Slow-Start for TCP with Large Congestion Windows*), and Global Synchronization (as described in **RFC 2884**):

Queue management algorithms traditionally manage the length of packet queues in the router by dropping packets only when the buffer overflows. A maximum length for each queue is configured. The router will accept packets till this maximum size is exceeded, at which point it will drop incoming packets. New packets are accepted when buffer space allows. This technique is known as Tail Drop. This method has served the Internet well for years, but has the several drawbacks. Since all arriving packets (from all flows) are dropped when the buffer overflows, this interacts badly with the congestion control mechanism of TCP. A cycle is formed with a burst of drops after the maximum queue size is exceeded, followed by a period of underutilization at the router as end systems back off. End systems then increase their windows simultaneously up to a point where a burst of drops happens again. This phenomenon is called Global Synchronization. It leads to poor link utilization and lower overall throughput. Another problem with Tail Drop is that a single connection or a few flows could monopolize the queue space, in some circumstances. This results in a lock out phenomenon leading to synchronization or other timing effects. Lastly, one of the major drawbacks of Tail Drop is that queues remain full for long periods of time. One of the major goals of queue management is to reduce the steady state queue size.

## Algorithm for Outbound Bandwidth Management

Each packet through the SonicWALL is initially classified as either a **Real Time** or a **Firewall** packet. Firewall packets are user-generated packets that always pass through the BWM module. Real time packets are usually firewall generated packets that are not processed by the BWM module, and are implicitly given the highest priority. Real Time (firewall generated) packets include:

- WAN Load Balancing Probe
- ISAKMP
- Web CFS
- PPTP and L2TP control packets
- DHCP
- ARP Packets
- Web Sense
- Syslog
- NTP
- Security Services (AV, signature updates, license manager)

## Outbound BWM Packet Processing Path

- a. Determine that the packet is bound for the WAN Zone.
- b. Determine that the packet is classifiable as a Firewall packet.
- c. Match the packet to an Access Rule to determine BWM setting.
- d. Queue the packet in the appropriate rule queue.

## Guaranteed Bandwidth Processing

This algorithm depicts how all the policies use up the GBW.

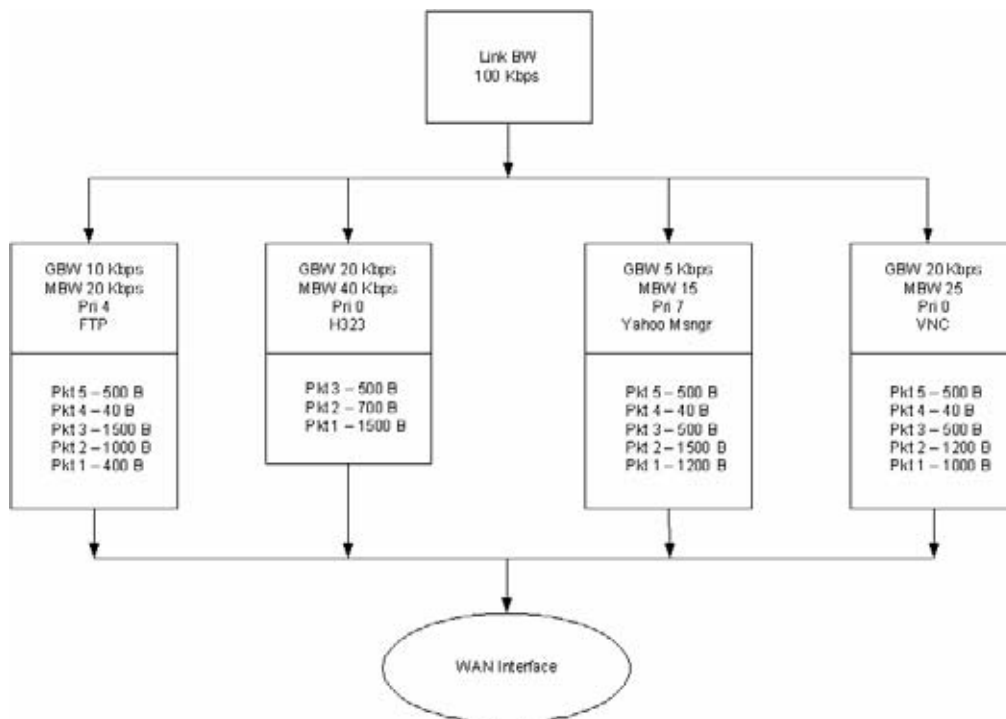
- a. Start with a link credit equal to available link BW.
- b. Initialize the class credit with configured GBW for the rule.
- c. If that packet length is less than or equal to the class credit, transmit the packet and deduct the length from class credit and link credit.
- d. Choose the next packet from queue and repeat step c until class credit is lesser or rule queue is empty.
- e. Choose the next rule queue and repeat steps b through d.

## Maximum Bandwidth Processing

This algorithm depicts how the unutilized link BW is used up by the policies. We start with the highest priority ring and transmit packets from all the rule queues in a round robin fashion until link credit is exhausted or all queues are empty. Then we move on to the next lowest priority ring and repeat the same.

- a. Start with the link credit equal to the left over link BW after GBW utilization.
- b. Choose the highest priority ring.
- c. Initialize class credit to (MBW - GBW).
- d. Check if the length of a packet from the rule queue is below class credit as well as link credit.
- e. If yes, transmit the packet and deduct the length from class credit and link credit.
- f. Choose the next rule queue and repeat steps c through f until link credit gets exhausted or this priority ring has all its queues empty.
- g. Choose the next lowest priority ring and repeat steps c through f.

## Example of Outbound BWM



The above diagram shows 4 policies are configured for OBWM with a link capacity of 100 Kbps. This means that the link capacity is 12800 Bytes/sec. Below table gives the BWM values for each rule in Bytes per second.

BWM values	FTP	H323	Yahoo Messenger	VNC
GBW	1280	2560	640	2560
MBW	2560	5120	1920	3200

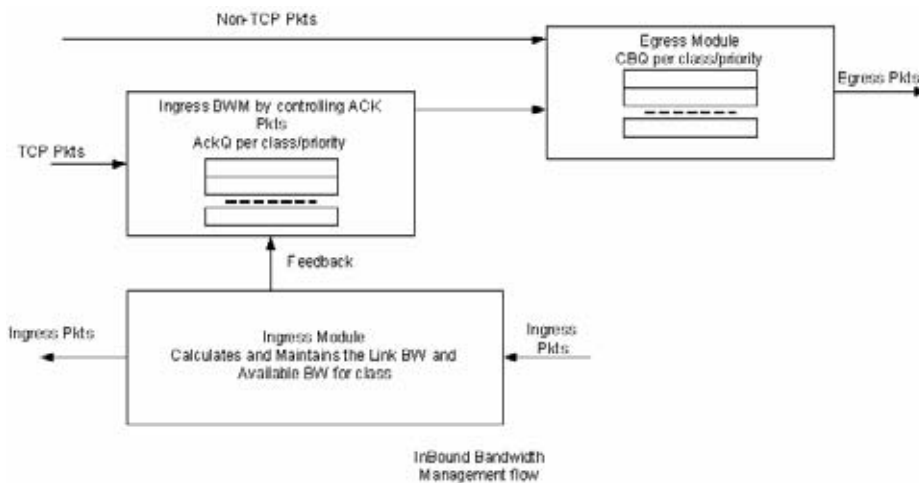
- a. For GBW processing, we start with the first queue in the rule queue list which is FTP. Link credit is 12800 and class credit is 1280. Pkt1 of 400B is sent out on the WAN link and link credit becomes 12400 and class credit becomes 880. Pkt2 is not sent out because there is not enough class credit to send 1500 Bytes. The remaining class credit is carried over to the next time slice.
- b. We move on to the next rule queue in this list which is for H323. Pkt1 of 1500B is sent out and link credit becomes 10900 and class credit for H323 becomes 1060. Pkt2 is also sent from queue hence link credit = 10200 and class credit = 360. Pkt3 is not sent since there is not enough class credit. The remaining class credit is carried over to the next time slice.
- c. Now we move onto Yahoo Messenger queue. Since Pkt1 cannot be accommodated with its class credit of 640 Bytes, no packets are processed from this queue. However, its class credit is carried over to the next time slice.
- d. From VNC queue, Pkt1 and Pkt2 are sent out leaving link credit = 8000 and class credit = 360. Class credit is carried over.
- e. Since all the queues have been processed for GBW we now move onto use up the left over link credit of 8000.

- f. Start off with the highest priority ring 0 and process all queues in this priority in a round robin fashion. H323 has Pkt3 of 500B which is sent since it can use up to max = 2560 (MBW-GBW). Now Link credit = 7500 and max = 2060.
- g. Move to the next queue in this priority ring which is VNC queue. Pkt3 of 500B is sent out leaving link credit = 7000B and class max = 140 (MBW-GBW - 500).
- h. Move to the next queue in this priority ring. Since H323 queue is empty already we move to the next queue which is VNC again.
- i. From VNC queue Pkt4 of 40B is sent out leaving link credit = 6960 and class max = 100. Pkt5 of 500B is not sent since class max is not enough.
- j. Now we move onto next lower priority queue. Since priority rings 1 through 3 are empty we choose priority ring 4 which has the rule queue for FTP. Pkt2 of 1000B is sent which leaves with link credit = 6000 and class max = 280. Since there are no other queues in this priority, FTP queue is processed again. But since class max is not enough for Pkt3 of 1500B it is not sent.
- k. Move to the next lower priority ring which is 7 for Yahoo Messenger. Pkt1 of 1200B is sent leaving link credit = 4800 and class max = 80. Since no other queues exist in this priority, this queue is processed again. Pkt2 of 1500B is not sent since it cannot be accommodated with max = 80.
- l. At this point, all the queues under all priority rings are processed for the current time slice.

## Inbound Bandwidth Management

Inbound BWM can be used to shape inbound TCP and UDP traffic. TCP's intrinsic flow control behavior is used to manage ingress bandwidth. To manage inbound UDP traffic, CBQ is used by the ingress module to queue the incoming packets. TCP rate is inherently controlled by the rate of receipt of ACKs; i.e. TCP sends out packets out on the network at the same rate as it receives ACKs. For IBWM, the sending rate of a TCP source will be reduced by controlling the rate of ACKs to the source. By delaying an ACK to the source, round-trip time (RTT) for the flow is increased, thus reducing the source's sending rate.

An ingress module monitors and records the ingress rate for each traffic class. It also monitors the egress ACKs and queues them if the ingress rate has to be reduced. According to ingress BW availability and average rate, the ACKs will be released.



## Algorithm for Inbound Bandwidth Management

IBWM maintains eight priority rings, where each priority ring has one queue for a rule that has IBWM enabled. The IBWM pool is processed from the highest to lowest priority ring further shaping the traffic. IBWM employs three key algorithms:

### Ingress Rate Update

This algorithm processes each packet from the WAN and updates the ingress rate of the class to which it belongs. It also marks the traffic class if it has over utilized the link.

- a. Determine that the packet is from the WAN zone and is a firewall packet.
- b. Add the packet length to the sum of packet lengths received so far in the current time slice. Deduct the minimum of (GBW, packet length) from link's credit.
- c. If the sum is greater than the class's credit, mark the class to be over utilizing the link.
- d. If the packet length is greater than the link's credit, mark the link as well as the class to be over utilized.

### Egress ACK monitor

This algorithm depicts how the egress ACKs are monitored and processed.

- a. Determine that the packet is to the WAN zone and is a TCP ACK.
- b. If class or interface is marked as over utilizing, queue the packet in the appropriate ingress rule queue.

### Process ACKs

This algorithm is used to update the BW parameters per class according to the amount of BW usage in the previous time slice. Amount of BW usage is given by the total number of bytes received for the class in the previous time slice. The algorithm is also used to process the packets from the ingress module queues according to the available credit for the class.

## Credit-Based Processing

A class will be in debt when its BW usage is more than the GBW for a particular time slice. All the egress ACKs for the class are then queued until the debt is reduced to zero. At each successive time slice, debt is deducted by GBW and if link BW is left, (MBW – GBW) is also deducted.

Compute BW usage in the previous time slice:

- a. Compute average ingress rate using the amount of BW usage by the class.
- b. If the BW usage is more than the class credit, record the difference as debt. If link BW is left over, deduct (MBW - GBW) from debt.
- c. Compute the class and link credit for the current time slice:
  - If the class is in debt, deduct GBW from debt and also from link's credit, indicating that the class has already used up its GBW for the current time slice.
  - If class is not in debt and there are packets arriving for this class, accumulate link credit; i.e. add GBW to credit at each time slice.
  - Class is marked as over utilizing if debt is nonzero.
- d. Process packets from ingress pool from highest priority ring to lowest priority ring.

- e. Record class credit as remaining credit.
- f. If remaining credit is greater than or equal to average rate, process the ACK packet and deduct average rate from remaining credit.
- g. Repeat g until remaining credit is not enough or the ingress ACK queue is empty.
- h. Repeat steps f through h for the next rule queue in the ring.
- i. Repeat steps f through i for the next lowest priority ring.

## Example of Inbound Bandwidth Management

Consider a class with GBW = 5 Kbps, MBW = 10 Kbps and Link BW = 100 Kbps. In terms of bytes per second we have GBW=640, excess BW = (MBW - GBW) = 640 and link BW = 12800.

No.	Ingress	Egress	Credit	Debt	Rate	Link BW	#Acks
1.	0	0	640	0	0	12800	0
2.	1300	0	620	0	1300	12780	0
2a.	0	40	620	0	1300	12780	1
3.	0	0	1260	0	1300	12800	1
4.	0	0	1900	0	1300	12800	0

- a. Class credit starts with 640. In row 2, 1300 bytes are received for this class in the previous time slice. Since it is more than the class credit, debt = 20 (1300-GBW-excess BW). For the current time slice class credit = 620 (GBW - debt), debt = 0 and link BW = 12780 since 20 bytes of debt is already used up from GBW for the class.
- b. Row 2a shows an egress ACK for the class. Since class credit is less than the rate this packet is queued in the appropriate ingress queue. And it will not be processed until class credit is at least equal to the rate.
- c. In the following time slices, class credit gets accumulated until it matches the rate. Hence, after two time slices class credit becomes 1900 (620 + 640 + 640). The queued ACK packet is process from the ingress pool at this point.

In row 2a, an ACK packet is received that needs to be sent to the TCP source on the WAN zone. Sending this ACK immediately would have caused the TCP source to send more packets immediately. By queuing the ACK and sending it only after the class credit reaches the average rate, we have reduced the TCP's sending rate; i.e. by doing this we have slowed down the ingress rate.

## BWM with WAN load balancing

BWM with WAN load balancing works in the following manner:

- a. If two interfaces are configured as WAN and load balancing is NOT enabled, BWM is only applied to the primary WAN interface.
- b. If two interfaces are configured as WAN and load balancing is enabled:
  - For Active/Passive Failover, BWM is done only on the active WAN interface.
  - For Round Robin and Ratio options, link capacity is the sum of available BW for primary and secondary WAN interface and BWM is done on both interfaces.
  - For Spill Over option, link capacity is Primary's available BW and BWM is done on primary interface before the spill over occurs. And after the spill over occurs, the secondary interface's capacity is used and BWM is done on the secondary WAN interface.



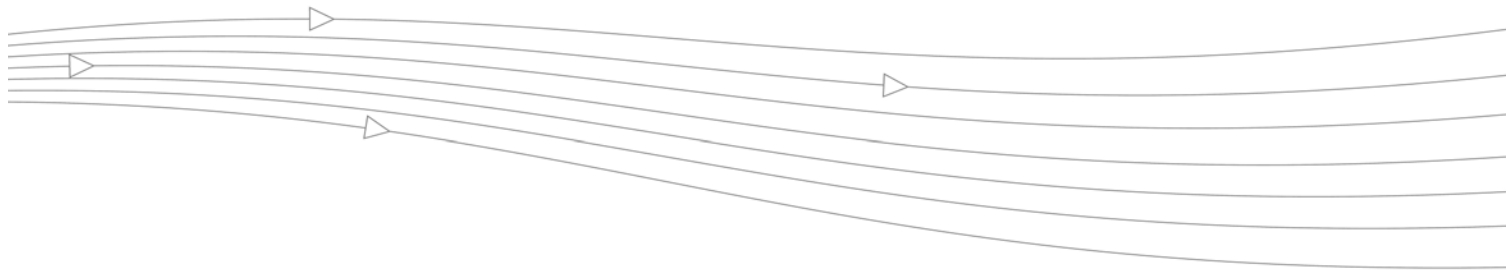
## Glossary

- **802.1p** – IEEE 802.1p is a Layer 2 (MAC layer) Class of Service mechanism that tags packets by using 3 priority bits (for a total of 8 priority levels) within the additional 16 bits of an 802.1q header. 802.1p processing requires compatible equipment for tag generation, recognition and processing, and should only be employed on compatible networks.
- **Bandwidth Management (BWM)** – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of outbound traffic, while policing often refers to the management of inbound traffic (also known as admission control). There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWALL employs a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic.
- **Class of Service (CoS)** – A designator or identifier, such as a layer 2 or layer 3 tag, that is applied to traffic after classification. CoS information will be used by the Quality of Service (QoS) system to differentiate between the classes of traffic on the network, and to provide special handling (e.g. prioritized queuing, low latency, etc.) as defined by the QoS system administrator.
- **Classification** – The act of identifying (or differentiating) certain types (or classes) of traffic. Within the context of QoS, this is performed for the sake of providing customized handling, typically prioritization or de-prioritization, based on the traffic's sensitivity to delay, latency, or packet loss. Classification within SonicOS Enhanced uses Access Rules, and can occur based on any or all of the following elements: source zone, destination zone, source address object, destination address object, service object, schedule object.
- **Code Point** – A value that is marked (or tagged) into the DSCP portion of an IP packet by a host or by an intermediate network device. There are currently 64 Code Points available, from 0 to 63, used to define the ascending prioritized class of the tagged traffic.
- **Conditioning** – A broad term used to describe a plurality of methods of providing Quality of Service to network traffic, including but not limited to discarding, queuing, policing, and shaping.
- **DiffServ** – Differentiated Services. A standard for differentiating between different types or classes of traffic on an IP network for the purpose of providing tailored handling to the traffic based on its requirements. DiffServ primarily depends upon Code Point values marked in the ToS header of an IP packet to differentiate between different classes of traffic. DiffServ service levels are executed on a Per Hop Basis at each router (or other DiffServ enabled network device) through which the marked traffic passes. DiffServ Service levels currently include at a minimum **Default**, **Assured Forwarding**, and **Expedited Forwarding**. Refer to the [“DSCP Marking” section on page 473](#) for more information.
- **Discarding** – A congestion avoidance mechanism that is employed by QoS systems in an attempt to predict when congestion might occur on a network, and to prevent the congestion by dropping over-limit traffic. Discarding can also be thought of as a queue management algorithm, since it attempts to avoid situations of full queues. Advanced discard mechanisms will abide by CoS markings so as to avoid dropping sensitive traffic. Common methods are:
  - **Tail Drop** – An indiscriminate method of dealing with a full queue wherein the last packets into the queue are dropped, regardless of their CoS marking.
  - **Random Early Detection (RED)** – RED monitors the status of queues to try to anticipate when a queue is about to become full. It then randomly discards packets in a staggered fashion to help minimize the potential of Global Synchronization. Basic implementations of RED, like Tail Drop, do not consider CoS markings.

- **Weighted Random Early Detection (WRED)** – An implementation of RED that factors DSCP markings into its discard decision process.
- **DSCP** – (Differentiate Services Code Points) – The repurposing of the ToS field of an IP header as described by RFC2747. DSCP uses 64 Code Point values to enable DiffServ (Differentiated Services). By marking traffic according to its class, each packet can be treated appropriately at every hop along the network.
- **Global Synchronization** – A potential side effect of discarding, the congestion avoidance method designed to deal with full queues. Global Synchronization occurs when multiple TCP flows through a congested link are dropped at the same time (as can occur in Tail Drop). When the native TCP slow-start mechanism commences with near simultaneity for each of these flows, the flows will again flood the link. This leads to cyclical waves of congestion and under-utilization.
- **Guaranteed Bandwidth** – A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of the total available bandwidth. SonicOS Enhanced 4.0 enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Guaranteed Bandwidth can also be set to 0%.
- **Inbound (Ingress or IBWM)** – The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of the ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **IntServ** – Integrated Services, as defined by RFC1633. An alternative CoS system to DiffServ, IntServ differs fundamentally from DiffServ in that it has each device request (or reserve) its network requirements before it sends its traffic. This requires that each hop on the network be IntServ aware, and it also requires each hop to maintain state information for every flow. IntServ is not supported by SonicOS. The most common implementation of IntServ is RSVP.
- **Maximum Bandwidth** – A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism to specify a bandwidth rate limit. SonicOS Enhanced 4.0 enhances the Bandwidth Management feature to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic. The Maximum Bandwidth can be set to 0%, which will prevent all traffic.
- **Outbound (Egress or OBWM)** – Conditioning the rate at which traffic is sent out an interface. Outbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.
- **Priority** – An additional dimension used in the classification of traffic. SonicOS uses 8 priority rings (0 = highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are serviced in the order of their priority ring.
- **Mapping** – Mapping, with regard to SonicOS' implementation of QoS, is the practice of converting layer 2 CoS tags (802.1p) to layer 3 CoS tags (DSCP) and back again for the purpose as preserving the 802.1p tags across network links that do not support 802.1p tagging. The map correspondence is fully user-definable, and the act of mapping is controlled by Access Rules.

- **Marking** – Also known as **tagging** or **coloring** – The act of applying layer 2 (802.1p) or layer 3 (DSCP) information to a packet for the purpose of differentiation, so that it can be properly classified (recognized) and prioritized by network devices along the path to its destination.
- **MPLS** - Multi Protocol Label Switching. A term that comes up frequently in the area of QoS, but which is natively unsupported by most customer premise IP networking devices, including SonicWALL appliances. MPLS is a carrier-class network service that attempts to enhance the IP network experience by adding the concept connection-oriented paths (Label Switch Paths – LSPs) along the network. When a packet leaves a customer premise network, it is tagged by a Label Edge Router (LER) so that the label can be used to determine the LSP. The MPLS tag itself resides between layer 2 and layer 3, imparting upon MPLS characteristics of both network layers. MPLS is becoming quite popular for VPNs, offering both layer 2 and layer 3 VPN services, but remains interoperable with existing IPsec VPN implementation. MPLS is also very well known for its QoS capabilities, and interoperates well with conventional DSCP marking.
- **Per Hop Behavior (PHB)** – The handling that will be applied to a packet by each DiffServ capable router it traverses, based upon the DSCP classification of the packet. The behavior can be among such actions as discard, re-mark (re-classify), best-effort, assured forwarding, or expedited forwarding.
- **Policing** – A facility of traffic conditioning that attempts to control the rate of traffic into or out of a network link. Policing methods range from indiscriminate packet discarding to algorithmic shaping, to various queuing disciplines.
- **Queuing** – To effectively make use of a link's available bandwidth, queues are commonly employed to sort and separately manage traffic after it has been classified. Queues are then managed using a variety of methods and algorithms to ensure that the higher priority queues always have room to receive more traffic, and that they can be serviced (de-queued or processed) before lower priority queues. Some common queue disciplines include:
  - **FIFO** – First In First Out. A very simple, undiscriminating queue where the first packet in is the first packet to be processed.
  - **Class Based Queuing (CBQ)** – A queuing discipline that takes into account the CoS of a packet, ensuring that higher priority traffic is treated preferentially.
  - **Weighted Fair Queuing (WFQ)** – A discipline that attempts to service queues using a simple formula based upon the packets' IP precedence and the total number of flows. WFQ has a tendency to become imbalanced when there is a disproportionately large number of high-priority flows to be serviced, often having the opposite of the desired effect.
  - **Token Based CBQ** – An enhancement to CBQ that employs a token, or a credit-based system that helps to smooth or normalize link utilization, avoiding burstiness as well as under-utilization. Employed by SonicOS' BWM.
- **RSVP** – Resource Reservation Protocol. An IntServ signaling protocol employed by some applications where the anticipated need for network behavior (e.g. delay and bandwidth) is requested so that it can be reserved along the network path. Setting up this Reservation Path requires that each hop along the way be RSVP capable, and that each agrees to reserve the requested resources. This system of QoS is comparatively resource intensive, since it requires each hop to maintain state on existing flows. Although IntServ's RSVP is quite different from DiffServ's DSCP, the two can interoperate. RSVP is not supported by SonicOS.

- **Shaping** – An attempt by a QoS system to modify the rate of traffic flow, usually by employing some feedback mechanism to the sender. The most common example of this is TCP rate manipulation, where acknowledgements (ACKs) sent back to a TCP sender are queued and delayed so as to increase the calculated round-trip time (RTT), leveraging the inherent behavior of TCP to force the sender to slow the rate at which it sends data.
- **Type of Service (ToS)** – A field within the IP header wherein CoS information can be specified. Historically used, albeit somewhat rarely, in conjunction with IP precedence bits to define CoS. The ToS field is now rather commonly used by DiffServ's code point values.



# CHAPTER 46

## Configuring SSL Control

---

### Firewall > SSL Control

This chapter describes how to plan, design, implement, and maintain the SSL Control feature. This chapter contains the following sections:

- [“Overview of SSL Control” section on page 493](#)
  - [“Key Features of SSL Control” section on page 495](#)
  - [“Key Concepts to SSL Control” section on page 496](#)
  - [“Caveats and Advisories” section on page 500](#)
- [“SSL Control Configuration” section on page 501](#)
- [“Enabling SSL Control on Zones” section on page 503](#)
- [“SSL Control Events” section on page 504](#)

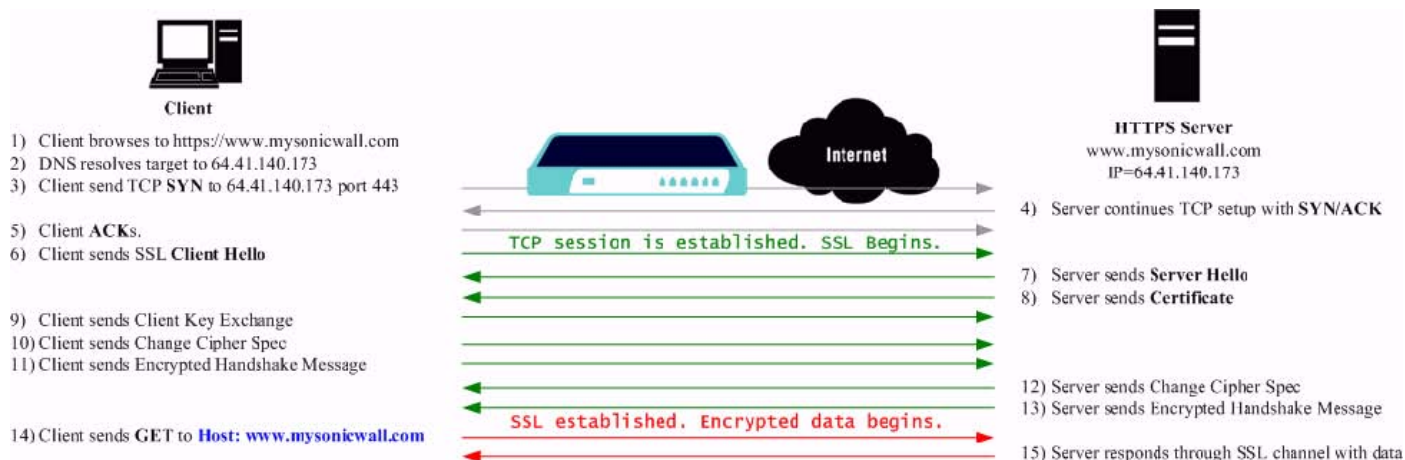
### Overview of SSL Control

This section provides an overview of SSL Control. It contains the following subsections:

- [“Key Features of SSL Control” section on page 495](#)
- [“Key Concepts to SSL Control” section on page 496](#)
- [“Caveats and Advisories” section on page 500](#)

SonicOS Enhanced 4.0 introduces SSL Control, a system for providing visibility into the handshake of SSL sessions, and a method for constructing policies to control the establishment of SSL connections. SSL (Secure Sockets Layer) is the dominant standard for the encryption

of TCP based network communications, with its most common and well-known application being HTTPS (HTTP over SSL). SSL provides digital certificate-based endpoint identification, and cryptographic and digest-based confidentiality to network communications.



An effect of the security provided by SSL is the obscuration of all payload, including the URL (Uniform Resource Locator, for example, <https://www.mysonicwall.com>) being requested by a client when establishing an HTTPS session. This is due to the fact that HTTP is transported within the encrypted SSL tunnel when using HTTPS. It is not until the SSL session is established (step 14, figure 1) that the actual target resource ([www.mysonicwall.com](http://www.mysonicwall.com)) is requested by the client, but since the SSL session is already established, no inspection of the session data by the firewall or any other intermediate device is possible. As a result, URL based content filtering systems cannot consider the request to determine permissibility in any way other than by IP address.

While IP address based filtering does not work well for unencrypted HTTP because of the efficiency and popularity of Host-header based virtual hosting (defined in Key Concepts below), IP filtering can work effectively for HTTPS due to the rarity of Host-header based HTTPS sites. But this trust relies on the integrity of the HTTPS server operator, and assumes that SSL is not being used for deceptive purposes.

For the most part, SSL is employed legitimately, being used to secure sensitive communications, such as online shopping or banking, or any session where there is an exchange of personal or valuable information. The ever decreasing cost and complexity of SSL, however, has also spurred the growth of more dubious applications of SSL, designed primarily for the purposes of obfuscation or concealment rather than security.

An increasingly common camouflage is the use of SSL encrypted web-based proxy servers for the purpose of hiding browsing details, and bypassing content filters. While it is simple to block well known HTTPS proxy services of this sort by their IP address, it is virtually impossible to block the thousands of privately-hosted proxy servers that are readily available through a simple web-search. The challenge is not the ever-increasing number of such services, but rather their unpredictable nature. Since these services are often hosted on home networks using dynamically addressed DSL and cable modem connections, the targets are constantly moving. Trying to block an unknown SSL target would require blocking all SSL traffic, which is practically infeasible.

SSL Control provides a number of methods to address this challenge by arming the security administrator with the ability to dissect and apply policy based controls to SSL session establishment. While the current implementation does not decode the SSL application data, it does allow for gateway-based identification and disallowance of suspicious SSL traffic.

## Key Features of SSL Control

Feature	Benefit
Common-Name based White and Black Lists	<p>The administrator can define lists of explicitly allowed or denied certificate subject common names (described in Key Concepts). Entries will be matched on substrings, for example, a blacklist entry for “prox” will match “www.megaproxy.com”, “www.proxify.com” and “proxify.net”. This allows the administrator to easily block all SSL exchanges employing certificates issued to subjects with potentially objectionable names. Inversely, the administrator can easily authorize all certificates within an organization by whitelisting a common substring for the organization. Each list can contain up to 1,024 entries.</p> <p>Since the evaluation is performed on the subject common-name embedded in the certificate, even if the client attempts to conceal access to these sites by using an alternative hostname or even an IP address, the subject will always be detected in the certificate, and policy will be applied.</p>
Self-Signed Certificate Control	<p>It is common practice for legitimate sites secured by SSL to use certificates issued by well-known certificate authorities, as this is the foundation of trust within SSL. It is almost equally common for network appliances secured by SSL (such as SonicWALL security appliances) to use self-signed certificates for their default method of security. So while self-signed certificates in closed-environments are not suspicious, the use of self-signed certificates by publicly or commercially available sites is. A public site using a self-signed certificate is often an indication that SSL is being used strictly for encryption rather than for trust and identification. While not absolutely incriminating, this sometimes suggests that concealment is the goal, as is commonly the case for SSL encrypted proxy sites.</p> <p>The ability to set a policy to block self-signed certificates allows security administrators to protect against this potential exposure. To prevent discontinuity of communications to known/trusted SSL sites using self-signed certificates, the whitelist feature can be used for explicit allowance.</p>
Untrusted Certificate Authority Control	<p>Like the use of self-signed certificates, encountering a certificate issued by an untrusted CA isn't an absolute indication of disreputable obscuration, but it does suggest questionable trust.</p> <p>SSL Control can compare the issuer of the certificate in SSL exchanges against the certificates in the SonicWALL's certificate store. The certificate store contains approximately 100 well-known CA certificates, exactly like today's web-browsers. If SSL Control encounters a certificate that was issued by a CA not in its certificate store, it can disallow the SSL connection.</p> <p>For organizations running their own private certificate authorities, the private CA certificate can easily be imported into the SonicWALL's certificate store to recognize the private CA as trusted. The store can hold up to 256 certificates.</p>

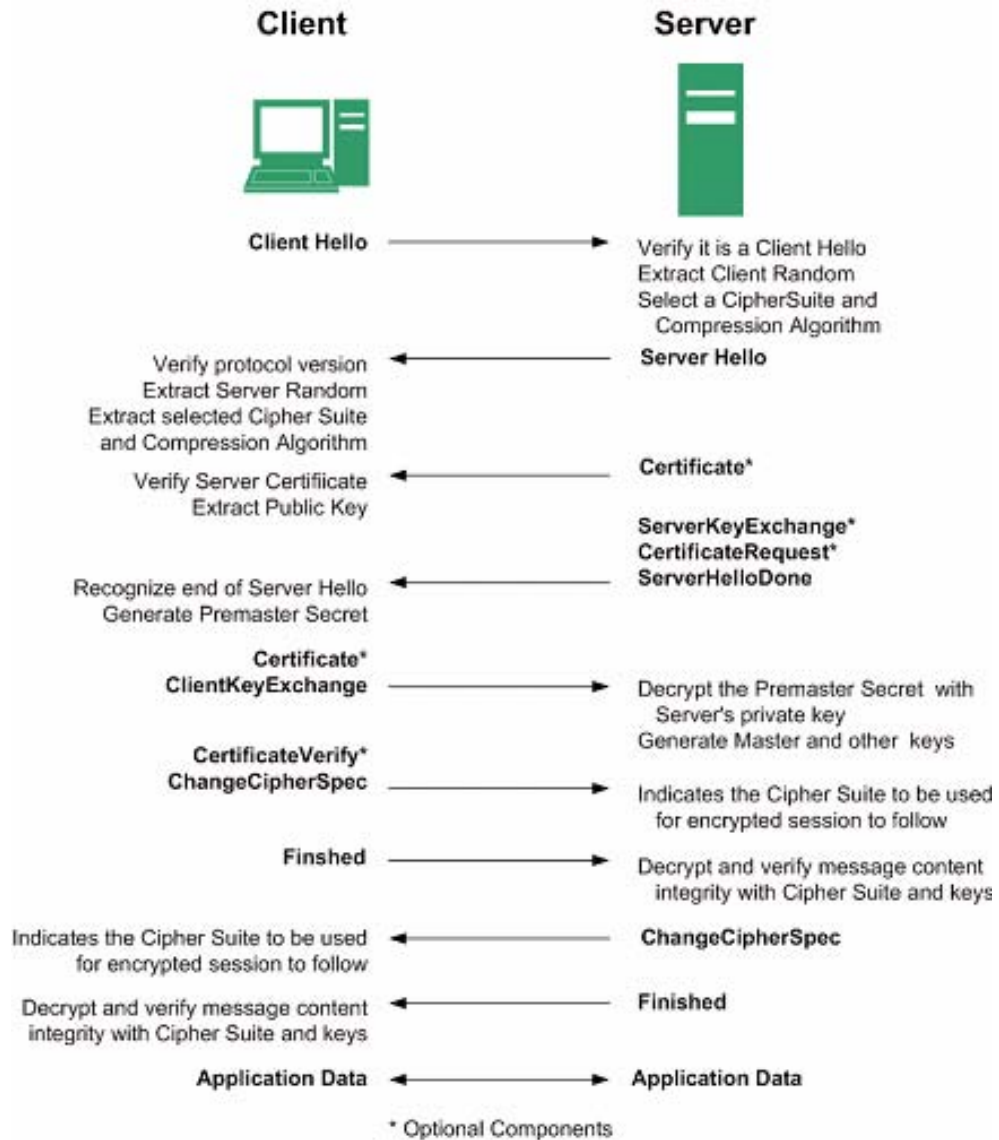
Feature	Benefit
SSL version, Cipher Strength, and Certificate Validity Control	SSL Control provides additional management of SSL sessions based on characteristics of the negotiation, including the ability to disallow the potentially exploitable SSLv2, the ability to disallow weak encryption (ciphers less than 64 bits), and the ability to disallow SSL negotiations where a certificate's date ranges are invalid. This enables the administrator to create a rigidly secure environment for network users, eliminating exposure to risk through unseen cryptographic weaknesses, or through disregard for or misunderstanding of security warnings.
Zone-Based Application	SSL Control is applied at the zone level, allowing the administrator to enforce SSL policy on the network. When SSL Control is enabled on the zone, the SonicWALL looks for Client Hellos sent from clients on that zone through the SonicWALL will trigger inspection. The SonicWALL then looks for the Server Hello and Certificate that is sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN Zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.
Configurable Actions and Event Notifications	When SSL Control detects a policy violation, it can log the event and block the connection, or it can simply log the event while allowing the connection to proceed.

## Key Concepts to SSL Control

- **SSL**- Secure Sockets Layer (SSL) is a network security mechanism introduced by Netscape in 1995. SSL was designed "to provide privacy between two communicating applications (a client and a server) and also to authenticate the server, and optionally the client." SSL's most popular application is HTTPS, designated by a URL beginning with https:// rather than simply http://, and it is recognized as the standard method of encrypting web traffic on the Internet. An SSL HTTP transfer typically uses TCP port 443, whereas a regular HTTP transfer uses TCP port 80. Although HTTPS is what SSL is best known for,



SSL is not limited to securing HTTP, but can also be used to secure other TCP protocols such as SMTP, POP3, IMAP, and LDAP. For more information, see [http://wp.netscape.com/eng/security/SSL\\_2.html](http://wp.netscape.com/eng/security/SSL_2.html). SSL session establishment occurs as follows:



- **SSLv2** – The earliest version of SSL still in common use. SSLv2 was found to have a number of weaknesses, limitations, and theoretical deficiencies (comparatively noted in the SSLv3 entry), and is looked upon with scorn, disdain, and righteous indignation by security purists.
- **SSLv3** – SSLv3 was designed to maintain backward compatibility with SSLv2, while adding the following enhancements:
  - Alternate key exchange methods, including Diffie-Hellman.
  - Hardware token support for both key exchange and bulk encryption.
  - SHA, DSS, and Fortezza support.
  - Out-of-Band data transfer.

- TLS – Transport Layer Security (version 1.0), also known as SSLv3.1, is very similar to SSLv3, but improves upon SSLv3 in the following ways:

SSL	TLS
Uses a preliminary HMAC algorithm	Uses HMAC as described in RFC 2104
Does not apply MAC to version info	Applies MAC to version info
Does not specify a padding value	Initializes padding to a specific value
Limited set of alerts and warning	Detailed Alert and Warning messages

- **MAC** – A MAC (Message Authentication Code) is calculated by applying an algorithm (such as MD5 or SHA1) to data. The MAC is a message digest, or a one-way hash code that is fairly easy to compute, but which is virtually irreversible. In other words, with the MAC alone, it would be theoretically impossible to determine the message upon which the digest was based. It is equally difficult to find two different messages that would result in the same MAC. If the receiver’s MAC calculation matches the sender’s MAC calculation on a given piece of data, the receiver is assured that the data has not been altered in transit.
- **Client Hello** – The first message sent by the client to the server following TCP session establishment. This message starts the SSL session, and consists of the following components:
  - **Version** – The version of SSL that the client wishes to use in communications. This is usually the most recent version of SSL supported by the client.
  - **Random** – A 32-bit timestamp coupled with a 28 byte random structure.
  - **Session ID** – This can either be empty if no Session ID data exists (essentially requesting a new session) or can reference a previously issued Session ID.
  - **Cipher Suites** – A list of the cryptographic algorithms, in preferential order, supported by the clients.
  - **Compression Methods** – A list of the compression methods supported by the client (typically null).
- **Server Hello** – The SSL server’s response to the Client Hello. It is this portion of the SSL exchange that SSL Control inspects. The Server Hello contains the version of SSL negotiated in the session, along with cipher, session ID and certificate information. The actual X.509 server certificate itself, although a separate step of the SSL exchange, usually begins (and often ends) in the same packet as the Server Hello.
- **Certificates** - X.509 certificates are unalterable digital stamps of approval for electronic security. There are four main characteristics of certificates:
  - Identify the subject of a certificate by a common name or distinguished name (CN or DN).
  - Contain the public key that can be used to encrypt and decrypt messages between parties
  - Provide a digital signature from the trusted organization (Certificate Authority) that issued the certificate.
  - Indicate the valid date range of the certificate
- **Subject** – The grantee of a certificate identified by a common name (CN). When a client browses to an SSL site, such as <https://www.mysonicwall.com>, the server sends its certificate which is then evaluated by the client. The client checks that the certificate’s dates are valid, that it was issued by a trusted CA, and that the subject CN matches the requested host name (i.e. they are both “www.mysonicwall.com”). Although a subject CN

mismatch elicits a browser alert, it is not always a sure sign of deception. For example, if a client browses to <https://mysonicwall.com>, which resolves to the same IP address as [www.mysonicwall.com](http://www.mysonicwall.com), the server will present its certificate bearing the subject CN of [www.mysonicwall.com](http://www.mysonicwall.com). An alert will be presented to the client, despite the total legitimacy of the connection.

- **Certificate Authority (CA)** - A Certificate Authority (CA) is a trusted entity that has the ability to sign certificates intended, primarily, to validate the identity of the certificate's subject. Well-known certificate authorities include VeriSign, Thawte, Equifax, and Digital Signature Trust. In general, for a CA to be trusted within the SSL framework, its certificate must be stored within a trusted store, such as that employed by most web-browsers, operating systems and run-time environments. The SonicOS trusted store is accessible from the **System > Certificates** page. The CA model is built on associative trust, where the client trusts a CA (by having the CA's certificate in its trusted store), the CA trusts a subject (by having issued the subject a certificate), and therefore the client can trust the subject.
- **Untrusted CA** – An untrusted CA is a CA that is not contained in the trusted store of the client. In the case of SSL Control, an untrusted CA is any CA whose certificate is not present in **System > Certificates**.
- **Self-Signed Certificates** – Any certificate where the issuer's common-name and the subject's common-name are the same, indicating that the certificate was self-signed.
- **Virtual Hosting** – A method employed by web-servers to host more than one web-site on a single server. A common implementation of virtual hosting is name-based (Host-header) virtual hosting, which allows for a single IP address to host multiple web-sites. With Host-header virtual hosting, the server determines the requested site by evaluating the "Host:" header sent by the client. For example, both [www.website1.com](http://www.website1.com) and [www.website2.com](http://www.website2.com) might resolve to 64.41.140.173. If the client sends a "GET /" along with "Host: [www.website1.com](http://www.website1.com)", the server can return content corresponding to that site.
- Host-header virtual hosting is generally not employed in HTTPS because the host header cannot be read until the SSL connection is established, but the SSL connection cannot be established until the server sends its Certificate. Since the server cannot determine which site the client will request (all that is known during the SSL handshake is the IP address) it cannot determine the appropriate certificate to send. While sending any certificate might allow the SSL handshake to commence, a certificate name (subject) mismatch will trigger a browser alert.
- **Weak Ciphers** – Relatively weak symmetric cryptography ciphers. Ciphers are classified as weak when they are less than 64 bits. For the most part, export ciphers are weak ciphers. The following is a list of common weak ciphers:

Cipher	Encryption	Occurs In
EXP1024-DHE-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-DES-CBC-SHA	DES (56)	SSLv3, TLS (export)
EXP1024-RC2-CBC-MD5	RC2(56)	SSLv3, TLS (export)
EDH-RSA-DES-CBC-SHA	DES (56)	SSLv3, TLS
EDH-DSS-DES-CBC-SHA	DES (56)	SSLv3, TLS
DES-CBC-SHA	DES (56)	SSLv2, SSLv3, TLS
EXP1024-DHE-DSS-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-SHA	RC4 (56)	SSLv3, TLS (export)
EXP1024-RC4-MD5	RC4 (56)	SSLv3, TLS (export)
EXP-EDH-RSA-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-EDH-DSS-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-DES-CBC-SHA	DES (40)	SSLv3, TLS (export)
EXP-RC2-CBC-MD5	RC2 (40)	SSLv2, SSLv3, TLS (export)
EXP-RC4-MD5	RC4 (40)	SSLv2, SSLv3, TLS (export)

## Caveats and Advisories

1. Self-signed and Untrusted CA enforcement – If enforcing either of these two options, it is strongly advised that you add the common names of any SSL secured network appliances within your organization to the whitelist to ensure that connectivity to these devices is not interrupted. For example, the default subject name of SonicWALL UTM appliances is “192.168.168.168”, and the default common name of SonicWALL SSL-VPN appliances is “192.168.200.1”.
2. If your organization employs its own private Certificate Authority (CA), it is strongly advised that you import your private CA’s certificate into the **System > Certificates** store, particularly if you will be enforcing blocking of certificates issued by untrusted CAs. Refer to the **System > Certificates** section of the SonicOS Enhanced Administrator’s Guide for more information on this process.
3. SSL Control inspection is currently only performed on TCP port 443 traffic. SSL negotiations occurring on non-standard ports will not be inspected at this time.
4. **Server Hello fragmentation** – In some rare instances, an SSL server will fragment the Server Hello. If this occurs, the current implementation of SSL Control will not decode the Server Hello. SSL Control policies will not be applied to the SSL session, and the SSL session will be allowed.
5. **Session termination handling** – When SSL Control detects a policy violation and terminates an SSL session, it will simply terminate the session at the TCP layer. Because the SSL session is in an embryonic state at this point, it is not currently possible to redirect the client, or to provide any kind of informational notification of termination to the client.
6. **Whitelist precedence** – The whitelist takes precedence over all other SSL Control elements. Any SSL server certificate which matches an entry in the whitelist will allow the SSL session to proceed, even if other elements of the SSL session are in violation of the configured policy. This is by design.
7. SonicOS Enhanced 4.0 increased the number of pre-installed (well-known) CA certificates from 8 to 93. The resulting repository is very similar to what can be found in most web-browsers. Other certificate related changes:
  - a. The maximum number of CA certificates was raised from 6 to 256.
  - b. The maximum size of an individual certificate was raised from 2,048 to 4,096.
  - c. The maximum number of entries in the whitelist and blacklist is 1,024 each.

## SSL Control Configuration

SSL Control is located on **Firewall** panel, under the **SSL Control** Folder. SSL Control has a global setting, as well as a per-zone setting. By default, SSL Control is not enabled at the global or zone level. The individual page controls are as follows (refer the Key Concepts for SSL Control section for more information on terms used below).

The screenshot shows the SSL Control configuration interface. At the top, there is a breadcrumb 'Firewall > SSL Control' and three buttons: 'Apply', 'Cancel', and a help icon '?'. Below this is the 'General Settings' section, which includes a checked checkbox for 'Enable SSL Control' and a note: 'Note: Enforce the SSL Control Service per zone from the [Network > Zones](#) page.' The 'Action' section has two radio buttons: 'Log the event' (unselected) and 'Block the connection and log the event' (selected). The 'Configuration' section contains seven checked checkboxes: 'Enable Blacklist', 'Enable Whitelist', 'Detect Expired Certificates', 'Detect SSLv2', 'Detect Self-Signed Certificates', 'Detect Certificate signed by an Untrusted CA', and 'Detect Weak Ciphers (<=64bits)'. The 'Custom Lists' section has the text 'Configure Blacklist and Whitelist' and a 'Configure...' button.

- **Enable SSL Control** – The global setting for SSL Control. This must be enabled for SSL Control applied to zones to be effective.
- **Log the event** – If an SSL policy violation, as defined within the Configuration section below, is detected, the event will be logged, but the SSL connection will be allowed to continue.
- **Block the connection and log the event** – In the event of a policy violation, the connection will be blocked and the event will be logged.
- **Enable Blacklist** – Controls detection of the entries in the blacklist, as configured in the Configure Lists section below.
- **Enable Whitelist** – Controls detection of the entries in the whitelist, as configured in the Configure Lists section below. Whitelisted entries will take precedence over all other SSL control settings.
- **Detect Expired Certificates** – Controls detection of certificates whose start date is before the current system time, or whose end date is beyond the current system time. Date validation depends on the SonicWALL's System Time. Make sure your System Time is set correctly, preferably synchronized with NTP, on the **System > Time** page.
- **Detect SSLv2** – Controls detection of SSLv2 exchanges. SSLv2 is known to be susceptible to cipher downgrade attacks because it does not perform integrity checking on the handshake. Best practices recommend using SSLv3 or TLS in its place.

- **Detect Self-signed certificates** – Controls the detection of certificates where both the issuer and the subject have the same common name.
- **Detect Certificates signed by an Untrusted CA** – Controls the detection of certificates where the issuer’s certificate is not in the SonicWALL’s **System > Certificates** trusted store.
- **Detect Weak Ciphers (<64 bits)** – Controls the detection of SSL sessions negotiated with symmetric ciphers less than 64 bits, commonly indicating export cipher usage.
- **Configure Blacklist and Whitelist** – Allows the administrator to define strings for matching common names in SSL certificates. Entries are case-insensitive, and will be used in pattern-matching fashion, for example:

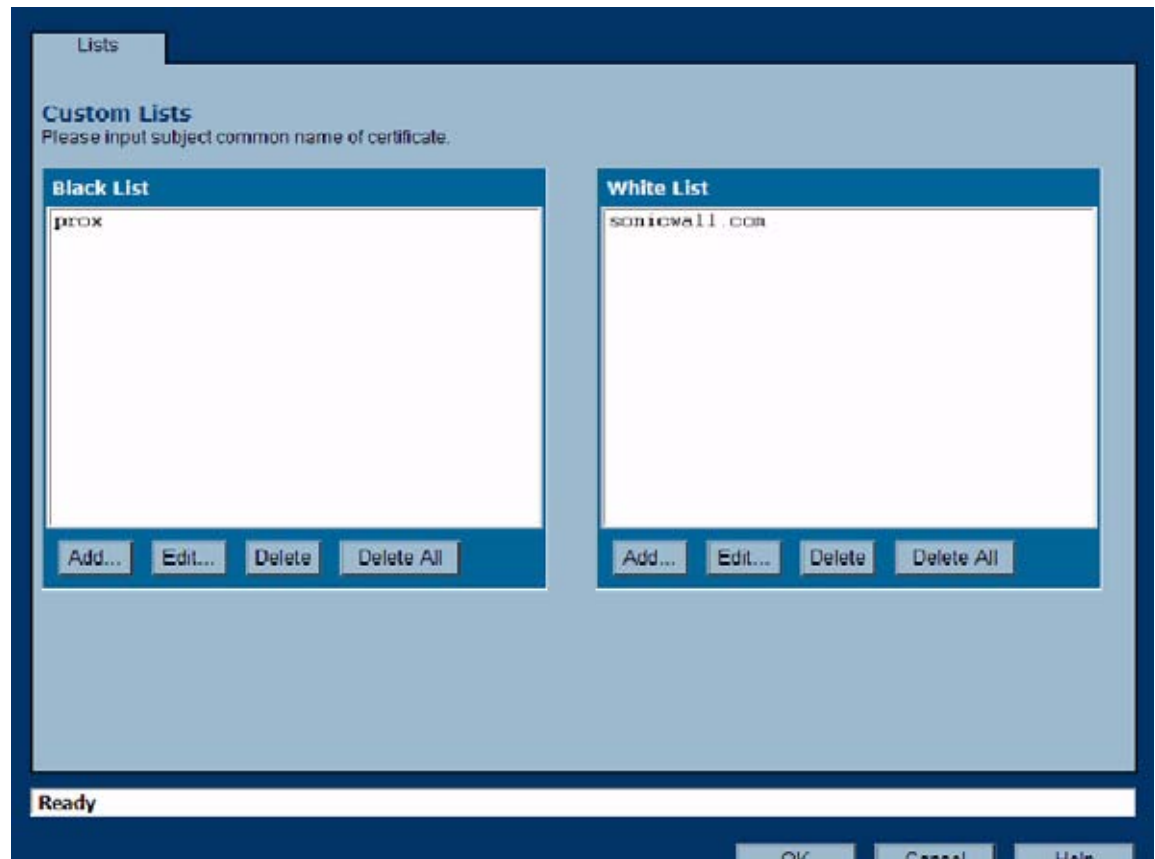
Entry	Will Match	Will Not Match
sonicwall.com	https://www.sonicwall.com, https:// csm.demo.sonicwall.com, https://mysonicwall.com, https:// supersonicwall.computers.org, https://67.115.118.87 <sup>a</sup>	https://www.sonicwall.de
prox	https://proxify.org, https:// www.proxify.org, https:// megaproxy.com, https:// 1070652204 <sup>b</sup>	https://www.freeproxy.ru <sup>c</sup>

a.67.115.118.67 is currently the IP address to which sslvpn.demo.sonicwall.com resolves, and that site uses a certificate issued to sslvpn.demo.sonicwall.com. This will result in a match to “sonicwall.com” since matching occurs based on the common name in the certificate.

b.This is the decimal notation for the IP address 63.208.219.44, whose certificate is issued to www.megaproxy.com.

c.www.freeproxy.ru will not match “prox” since the common name on the certificate that is currently presented by this site is a self-signed certificate issued to “-“. This can, however, easily be blocked by enabling control of self-signed or Untrusted CA certificates.

To configure the Whitelist and Blacklist, click the **Configure** button to bring up the following window.



Entries can be added, edited and deleted with the buttons beneath each list window.



**Note**

List matching will be based on the subject common name in the certificate presented in the SSL exchange, not in the URL (resource) requested by the client.

Changes to any of the SSL Control settings will not affect currently established connections; only new SSL exchanges that occur following the change commit will be inspected and affected.

## Enabling SSL Control on Zones

Once SSL Control has been globally enabled, and the desired options have been configured, SSL Control must be enabled on one or more zones. When SSL Control is enabled on the zone, the SonicWALL looks for Client Hellos sent from clients on that zone through the SonicWALL will trigger inspection. The SonicWALL then looks for the Server Hello and Certificate that is

sent in response for evaluation against the configured policy. Enabling SSL Control on the LAN Zone, for example, will inspect all SSL traffic initiated by clients on the LAN to any destination zone.

**Note**

If you are activating SSL Control on a zone (for example, the LAN zone) where there are clients who will be accessing an SSL server on another zone connected to the SonicWALL (for example, the DMZ zone) it is recommended that you add the subject common name of the that server's certificate to the whitelist to ensure continuous trusted access.

To enable SSL Control on a zone, browse to the **Network > Zones** page, and select the configure icon for the desired zone. In the Edit Zone window, select the Enable SSL Control checkbox, and click OK. All new SSL connections initiated from that zone will now be subject to inspection.

## SSL Control Events

The following log entries illustrate and describe the possible SSL Control events:

Log View								Items 1 to 10 (of 10) < >
#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	09/21/2034 15:08:27.032	Info	Network Access	SSL Control: Certificate with invalid date	199.67.185.5, 443, X1	10.50.165.17, 60627, X0	HTTPS Access Denied: www.smithbarney.com	
2	09/21/2034 15:08:27.032	Info	Network Access	SSL Control: Certificate chain not complete	199.67.185.5, 443, X1	10.50.165.17, 60627, X0	www.smithbarney.com	
3	09/21/2006 15:00:19.880	Info	Network Access	SSL Control: Self-signed certificate	192.168.0.2, 443, X1 (admin)	10.50.165.17, 59123, X0	HTTPS Access Denied: mySSLVPN.moosifer.com	
4	09/21/2006 14:57:08.384	Info	Network Access	SSL Control: Untrusted CA	192.168.0.2, 443, X1 (admin)	10.50.165.17, 59122, X0	HTTPS Access Denied: Cert CN:mySSLVPN.moosifer.com; CA:mySSLVPN.moosifer.com	
5	09/21/2006 14:51:14.400	Info	Network Access	SSL Control: Website found in blacklist	63.208.219.44, 443, X1	10.50.165.17, 60627, X0	HTTPS Access Denied: www.megaproxy.com	
6	09/21/2006 14:50:44.944	Info	Network Access	SSL Control: Weak cipher being used	151.151.13.133, 443, X1	10.50.165.17, 49701, X0	HTTPS Access Denied: www.wellsfargo.com	
7	09/21/2006 14:50:44.928	Info	Network Access	SSL Control: Certificate chain not complete	151.151.13.133, 443, X1	10.50.165.17, 49701, X0	www.wellsfargo.com	
8	09/21/2006 14:49:25.752	Info	Network Access	SSL Control: Failed to decode Server Hello	204.180.153.231, 443, X1	10.50.165.17, 33335, X0		
9	09/21/2006 14:49:11.448	Info	Network Access	SSL Control: Website found in whitelist	67.115.118.67, 443, X1	10.50.165.17, 39311, X0	sslvpn.demo.sonicwall.com	
10	09/21/2006 14:48:52.176	Info	Network Access	SSL Control: HTTPS via SSL2	72.21.206.5, 443, X1	10.50.165.17, 49407, X0	HTTPS Access Denied: www.amazon.com	



Log events will include the client's username in the notes section (not shown) if the user logged in manually, or was identified through CIA/Single Sign On. If the user's identity is not available, the note will indicate that the user is *Unidentified*.

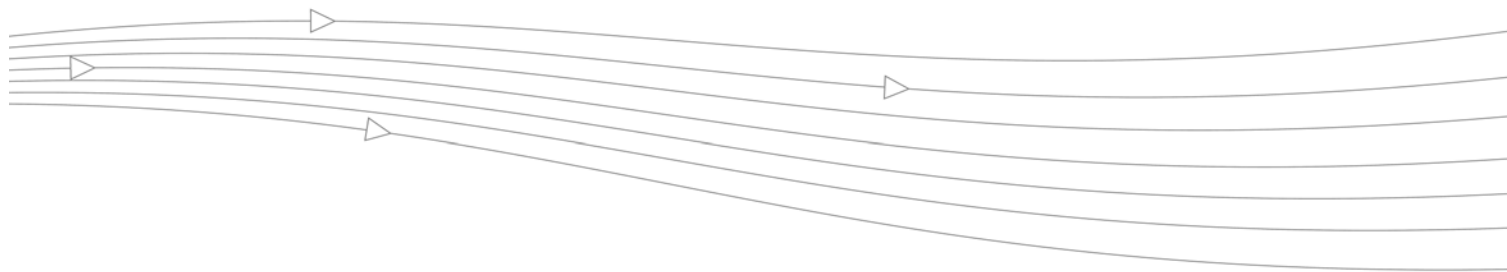
#	Event Message	Occurs When
1	SSL Control: Certificate with invalid date	The certificate's start date is before the SonicWALL's system time, or when the end date is after the system time. Note that for this illustration, the system time of the SonicWALL was set well into the future. Smithbarney.com is just peachy.
2	SSL Control: Certificate chain not complete	The certificate has been issued by an intermediate CA (chained certificate authority) with a trusted top-level CA, but the SSL server did not present the intermediate certificate. This log event is informational, and does not affect the SSL connection.
3	SSL Control: Self-signed certificate	The certificate being presented is self-signed, in other words, a certificate where the CN of the issuer and the subject match. <b>Note:</b> See entry #1 in the Caveats and Advisories section for information about enforcing self-signed certificate controls.
4	SSL Control: Untrusted CA	The certificate being presented has been issued by a CA that is not in the <b>System &gt; Certificates</b> store of the SonicWALL. <b>Note:</b> See entry #2 in the Caveats and Advisories section for information about enforcing untrusted CA controls.
5	SSL Control: Website found in blacklist	The common name of the subject matched a pattern entered into the blacklist. In this example, the pattern "prox" was entered, and the certificate presented was issued to the subject "www.megaproxy.com" matched, triggering the violation.
6	SSL Control: Weak cipher being used	The symmetric cipher being negotiated was less than 64 bits. In this example, the cipher DES-CBC-SHA was negotiated. Refer to the table in the Weak Ciphers entry of Key Concepts to SSL Control section for a list of weak ciphers.
7	See #2	See #2
8	SSL Control: Failed to decode Server Hello	The Server Hello from the SSL server was undecipherable. Also occurs when the Certificate and Server Hello are in different packets, as will be the case when connecting to SSL server on SonicWALL UTM (firewall and CSM) appliances. This log event is informational, and does not affect the SSL connection.
9	SSL Control: Website found in whitelist	The common name of the subject (typically a website) matched a pattern entered into the whitelist. Whitelist entries are always allowed, even if there are other policy violations in the negotiation, such as SSLv2 or weak-ciphers. In this example, the pattern "sonicwall.com" was entered, and the certificate presented was issued to "ssmvpn.demo.sonicwall.com"
10	SSL Control: HTTPS via SSLv2	The SSL session was being negotiated using SSLv2. SSLv2 is known to be susceptible to certain types of man-in-the-middle attacks. Best practices recommend using SSLv3 or TLS in its place.



# **PART 8**

# **VoIP**





# CHAPTER 47

## Configuring VoIP Support

---

### VoIP

This chapter contains the following sections:

- “VoIP Overview” on page 509
- “SonicWALL’s VoIP Capabilities” on page 512
- “Configuring SonicWALL VoIP Features” on page 520
- “VoIP Deployment Scenarios” on page 531

### VoIP Overview

This section provides an overview of VoIP. It contains the following sections:

- “What is VoIP?” on page 509
- “VoIP Security” on page 510
- “VoIP Protocols” on page 511

### What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

## VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

### Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. SonicWALL security appliances are VoIP enabled firewalls that eliminate the need for an SBC on your network.

## VoIP Protocols

VoIP technologies are built on two primary protocols, H.323 and SIP.

### H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It's a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
  - Address translation.
  - Registration, admission control, and status (RAS).
  - Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

### SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports 'presence' and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.

- **Redirect Server** - Responds to request but does not forward requests.
- **Registration Server** - Handles UA authentication and registration.

## SonicWALL's VoIP Capabilities

The following sections describe SonicWALL's integrated VoIP service:

- "VoIP Security" on page 512
- "VoIP Network" on page 513
- "VoIP Network Interoperability" on page 513
- "Supported VoIP Protocols" on page 514
- "How SonicOS Handles VoIP Calls" on page 517

### VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. SonicWALL security appliances detect and discard malformed and invalid packets before they reach their intended target.
- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. SonicWALL extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
  - Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
  - Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
  - Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Encrypted VoIP Device Support** - SonicWALL supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPsec VPNs to protect VoIP calls.
- **Application-Layer Protection** - SonicWALL delivers full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). SonicWALL IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in SonicWALL's Deep Packet Inspection engine



also provides proactive defense against newly discovered application and protocol vulnerabilities. Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

## VoIP Network

- **VoIP over Wireless LAN (WLAN)** - SonicWALL extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices attached to a wired network behind a SonicWALL are also provided to VoIP devices using a wireless network.



Note

---

SonicWALL's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks. Refer to the SonicWALL Secure Wireless Network Integrated Solutions Guide available on the SonicWALL Web site <http://www.sonicwall.com> for complete information.

---

- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into SonicWALL Quality of Service (QoS) features to provide predictability that is vital for certain types of applications.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary or backup WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.
- **High availability** - High availability is provided by SonicOS hardware failover, which ensures reliable, continuous connectivity in the event of a system failure.

## VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a SonicWALL security appliance.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicOS tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.

Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.

- **Validation of headers for all media packets** - SonicOS examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, SonicWALL provides protection for the entire VoIP session.
- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.
- **SonicOS allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicOS can block unauthorized and spam calls. This allows the administrator to be sure that the VoIP network is being used only for those calls authorized by the company.
- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS offers extensive monitoring and troubleshooting tools:
  - Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
  - Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
  - Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. SonicWALL ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.

## Supported VoIP Protocols

SonicWALL security appliances support transformations for the following protocols.

### H.323

SonicOS provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The SonicWALL DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicOS supports VoIP devices using the following additional ITU standards:
  - T.120 for application sharing, electronic white-boarding, file exchange, and chat
  - H.239 to allow multiple channels for delivering audio, video and data
  - H.281 for Far End Camera Control (FECC)

## SIP

SonicOS provides the following support for SIP:

- Base SIP standard (both RFC 2543 and RFC 3261)
- SIP INFO method (RFC 2976)
- Reliability of provisional responses in SIP (RFC 3262)
- SIP specific event notification (RFC 3265)
- SIP UPDATE method (RFC 3311)
- DHCP option for SIP servers (RFC 3361)
- SIP extension for instant messaging (RFC 3428)
- SIP REFER method (RFC 3515)
- Extension to SIP for symmetric response routing (RFC 3581)

## SonicWALL VoIP Vendor Interoperability

The following is a partial list of devices from leading manufacturers with which SonicWALL VoIP interoperates.

H.323	SIP
Soft-Phones:	Soft-Phones:
Avaya	Apple iChat
Microsoft NetMeeting	Avaya
OpenPhone	Microsoft MSN Messenger
PolyCom	Nortel Multimedia PC Client
SJLabs SJ Phone	PingTel Instant Xpressa
	PolyCom
Telephones/VideoPhones:	Siemens SCS Client SJLabs
Avaya	SJPhone
Cisco	XTen X-Lite
D-Link	Ubiquity SIP User Agent
PolyCom	
Sony	Telephones/ATAs:
	Avaya
Gatekeepers:	Cisco
Cisco	Grandstream BudgetOne
OpenH323 Gatekeeper	Mitel
	Packet8 ATA
Gateway:	PingTel Xpressa PolyCom
Cisco	PolyCom
	Pulver Innovations WiSIP
	SoundPoint
	SIP Proxies/Services:
	Cisco SIP Proxy Server
	Brekeke Software OnDo SIP Proxy
	Packet8
	Siemens SCS SIP Proxy
	Vonage

## CODECs

**SonicOS supports media streams from any CODEC** - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COderer/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:

- H.264, H.263, and H.261 for video
- MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

### VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on

SonicWALL security appliances do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

- Proprietary extensions to H.323 or SIP
- MGCP
- Megaco/H.248
- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG
- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

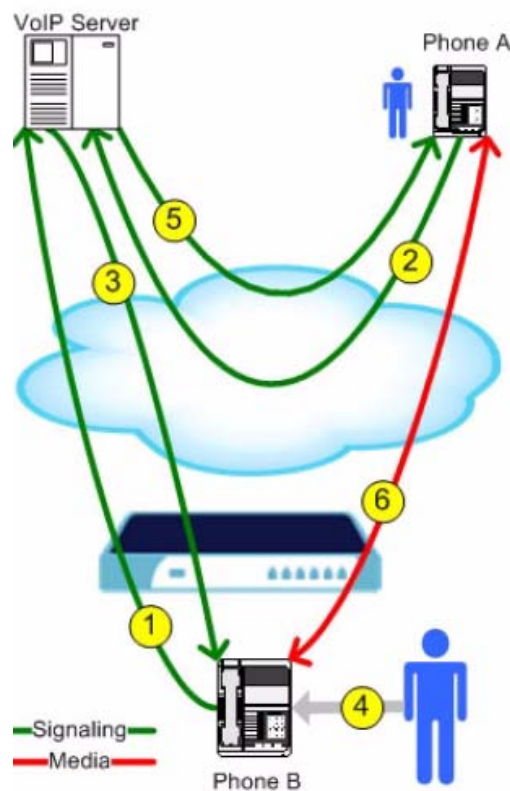
### How SonicOS Handles VoIP Calls

SonicOS provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicOS handles VoIP call flows.

#### Incoming Calls

The following figure shows the sequence of events that occurs during an incoming call.

**Figure 47:1 Incoming VoIP Call Flow**



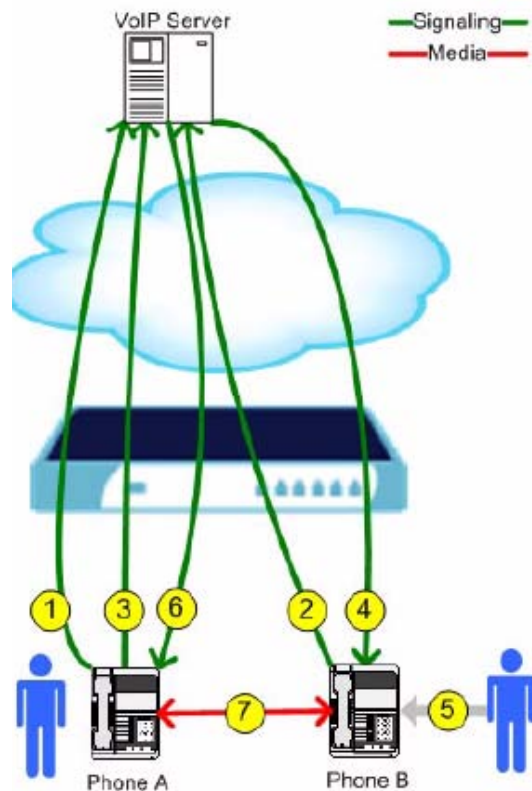
The following describes the sequence of events shown in Figure 42.1:

1. **Phone B registers with VoIP server** - The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.
2. **Phone A initiates a call to phone B** - Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicOS validates the source and content of the request. The firewall then determines phone B's private IP address.
4. **Phone B rings and is answered** - When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicOS translates this private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP server returns phone B media IP information to phone A** - Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.
6. **Phone A and phone B exchange audio/video/data through the VoIP server** - Using the internal database, SonicOS ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

## Local Calls

The following figure shows the sequence of events that occurs during a local VoIP call.

Figure 47:2 Local VoIP Call Flow



The following describes the sequence of events shown in Figure 42.2:

1. **Phones A and B register with VoIP server** - The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between the phones' private IP addresses and the firewall's public IP address. The VoIP server is unaware that the phones are behind a firewall. It associates the same IP address for both phones, but different port numbers.
2. **Phone A initiates a call to phone B by sending a request to the VoIP server** - Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the firewall's public IP address. The firewall then determines phone B's private IP address.
4. **Phone B rings and is answered** - When phone B is answered, the firewall translate its private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP Server returns phone B media IP information to phone A** - Both the called and calling party information within the messages are translated by SonicOS back to the private addresses and ports for phone A and phone B.
6. **Phone A and phone B directly exchange audio/video/data** - The SonicWALL security appliance routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the SonicWALL security appliance to perform address translation.

# Configuring SonicWALL VoIP Features

Configuring the SonicWALL security appliance for VoIP deployments builds on your basic network configuration in the SonicWALL management interface. This chapter assumes the SonicWALL security appliance is configured for your network environment.

## Supported Interfaces

VoIP devices are supported on the following SonicOS Zones:

- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

## Configuration Tasks

- “General VoIP Configuration” on page 521
  - “Configuring Consistent Network Address Translation (NAT)” on page 521
  - “Configuring SIP Settings” on page 522
  - “Configuring H.323 Transformations” on page 523
- “Configuring BWM and QoS” on page 523
  - “Bandwidth Management” on page 524
  - “Quality of Service” on page 524
  - “Configuring Bandwidth on the WAN Interface” on page 525
  - “Configuring VoIP Access Rules” on page 525
  - “Using the Public Server Wizard” on page 528
- “Configuring VoIP Logging” on page 531



## General VoIP Configuration

SonicOS includes the VoIP configuration settings on the **VoIP > Settings** page. This page is divided into three configuration settings sections: **General Settings**, **SIP Settings**, and **H.323 Settings**.

The screenshot shows the 'VoIP > Settings' configuration page. It has three main sections:

- General Settings:** Contains a checkbox for 'Enable consistent NAT' which is currently unchecked.
- SIP Settings:** Contains several options:
  - 'Enable SIP Transformations' is checked.
  - 'Permit non-SIP packets on signaling port' is unchecked.
  - 'Enable SIP Back-to-Back User Agent (B2BUA) support' is unchecked.
  - 'SIP Signaling inactivity time out (seconds):' is set to 1800.
  - 'SIP Media inactivity time out (seconds):' is set to 120.
  - 'Additional SIP signaling port (UDP) for transformations (optional):' is set to 0.
- H.323 Settings:** Contains several options:
  - 'Enable H.323 Transformations' is checked.
  - 'Only accept incoming calls from Gatekeeper' is unchecked.
  - 'Enable LDAP ILS Support' is unchecked.
  - 'H.323 SignalingMedia inactivity time out (seconds):' is set to 300.
  - 'Default WAN/DMZ Gatekeeper IP Address:' is set to 0.0.0.0.

### Configuring Consistent Network Address Translation (NAT)

Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair.

For example, NAT could translate the private (LAN) IP address and port pairs, 192.116.168.10/50650 and 192.116.168.20/50655 into public (WAN) IP/port pairs as follows:

Private IP/Port	Translated Public IP/Port
192.116.168.10/ 50650	64.41.140.167/40004
192.116.168.20/ 50655	64.41.140.167/40745

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in the previous result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

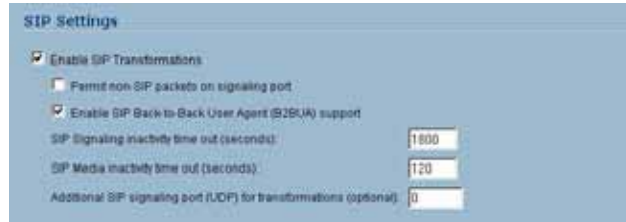
To enable Consistent NAT, select the **Enable Consistent NAT** setting and click **Apply**. This checkbox is disabled by default.



**Note**

Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.

## Configuring SIP Settings



By default, SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the SonicWALL security appliance and SIP clients are on the private (LAN) side behind the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

Selecting **Enable SIP Transformations** transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the SonicWALL security appliance to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWALL and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWALL. Selecting **Enable SIP Transformations** enables the SonicWALL to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformation** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select **Enable SIP Transformations** to transform the SIP messages.



Tip

In general, you should check the **Enable SIP Transformations** box unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic. This checkbox is disabled by default.

The **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be enabled when the SonicWALL security appliance can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN). This setting should only be enabled when the SIP Proxy Server is being used as a B2BUA.



Tip

If there is not the possibility of the SonicWALL security appliance seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

**SIP Signaling inactivity time out (seconds)** and **SIP Media inactivity time out (seconds)** define the amount of time a call can be idle (no traffic exchanged) before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **SIP Signaling inactivity time out** is 1800 seconds (30 minutes). The default time value for **SIP Media inactivity time out** is 120 seconds (2 minutes).

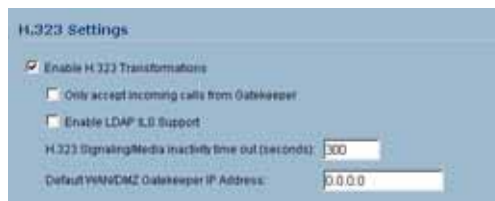
The **Additional SIP signaling port (UDP) for transformations** setting allows you to specify a non-standard UDP port used to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. Using this setting, the security appliance performs SIP transformation on these non-standard ports.



Tip

Vonage's VoIP service uses UDP port 5061.

## Configuring H.323 Transformations



Select **Enable H.323 Transformation** in the **H.323 Settings** section and click **Apply** to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWALL security appliance. The SonicWALL security appliance performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWALL security appliance.

Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper will refuse calls that fail authentication.

Select **Enable LDAP ILS Support** to enable Microsoft NetMeeting users to locate and connect to users for conferencing and collaboration over the Internet.

The **H.323 Signaling/Media inactivity time out (seconds)** field specifies the amount of time a call can be idle before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **H.323 Signaling/Media inactivity time out** is 300 seconds (5 minutes).

The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 224.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling.

## Configuring BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

SonicWALL's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

## Bandwidth Management

SonicOS offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) management interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public Zones (such as LAN and DMZ) destined to Untrusted and Encrypted Zones (such as WAN and VPN). Inbound bandwidth management can be applied to traffic sourced from Untrusted and Encrypted Zones destined to Trusted and Public Zones.

Enabling bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.

## Quality of Service

QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

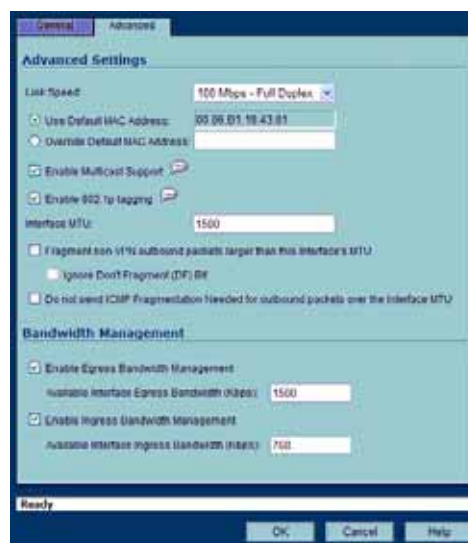
SonicOS includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.

**Note**

For more information on QoS and BWM, see “[Firewall > QoS Mapping](#)” section on page 467. Refer to the Configuring QoS and BWM Feature Module for complete BWM and QoS configuration instructions. Available on the SonicWALL Web site <[www.sonicwall.com/support/documentation.html](http://www.sonicwall.com/support/documentation.html)>

## Configuring Bandwidth on the WAN Interface

BWM configurations begin by enabling BWM on the relevant WAN interface, and specifying the interface's available bandwidth in Kbps. This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:



Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The bandwidth specified should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Bandwidth** tab will appear on Access Rules. See the following [“Configuring VoIP Access Rules”](#) section for more information.

To configure Bandwidth Management on the SonicWALL security appliance:

- Step 1** Select **Network > Interfaces**.
- Step 2** Click the Edit icon in the Configure column in the **WAN (X1)** line of the Interfaces table. The **Edit Interface** window is displayed.
- Step 3** Click the **Advanced** tab.
- Step 4** Check **Enable Egress (Outbound) Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Egress Bandwidth Management** field.
- Step 5** Check **Enable Ingress (Inbound) Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Ingress Bandwidth Management** field.
- Step 6** Click **OK**.

## Configuring VoIP Access Rules

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

If your SIP Proxy or H.323 Gateway is located behind the firewall, you can use the SonicWALL **Public Server Wizard** to automatically configure access rules.

**Tip**

Although custom rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.

**Note**

You must select Bandwidth Management on the **Network > Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

- Step 1** To add access rules for VoIP traffic on the SonicWALL security appliance: Go to the **Firewall > Access Rules** page, and under **View Style** click **All Rules**.
- Step 2** Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.

The screenshot shows the 'Add Rule' window in the SonicWALL management interface. The 'General' tab is active. The 'Action' is set to 'Allow'. The 'From Zone' is 'LAN' and the 'To Zone' is 'WAN'. The 'Service' is 'H323 Call Signaling'. The 'Source' is 'LAN Interface IP' and the 'Destination' is 'WAN Interface IP'. The 'Users Allowed' is 'All' and the 'Schedule' is 'Always on'. The 'Comment' is 'VoIP'. The 'Enable Logging' checkbox is checked, and the 'Allow Fragmented Packets' checkbox is unchecked. The status bar at the bottom of the window shows 'Ready'.

- Step 3** In the **General** tab, select **Allow** from the **Action** list to permit traffic.
- Step 4** Select the from and to zones from the **From Zone** and **To Zone** menus.
- Step 5** Select the service or group of services affected by the access rule from the **Service** list.
- For H.323, select one of the following or select **Create New Group** and add the following services to the group:
    - H.323 Call Signaling
    - H.323 Gatekeeper Discovery
    - H.323 Gatekeeper RAS

- For SIP, select **SIP**

**Step 6** Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.

**Step 7** If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type:** pulldown menu. Then enter the lowest and highest IP addresses in the range in the **Starting IP Address:** and **Ending IP Address** fields.

**Step 8** Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.

**Step 9** From the **Users Allowed** menu, add the user or user group affected by the access rule.

**Step 10** Select a schedule from the **Schedule** menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **system > Schedules** page.

**Step 11** Enter any comments to help identify the access rule in the **Comments** field.

**Step 12** Click the **Bandwidth** tab.

**Step 13** Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.

**Step 14** Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

**Step 15** Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.



**Tip**

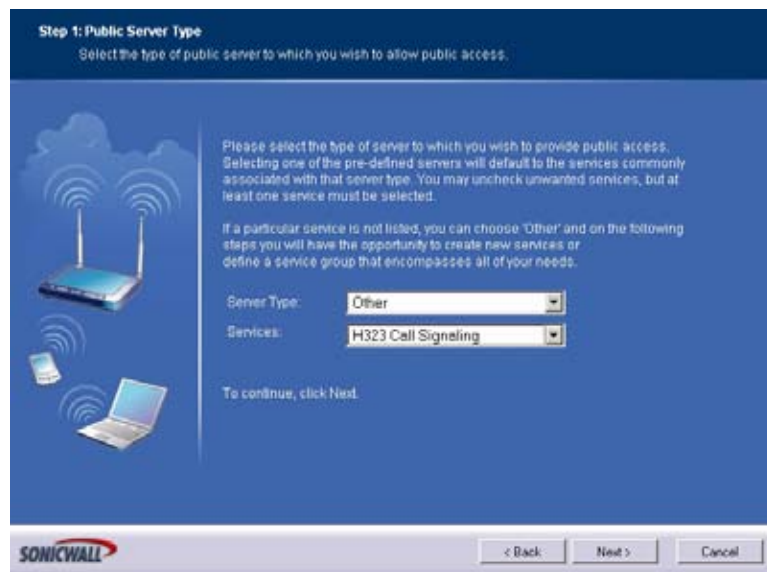
Rules using Bandwidth Management take priority over rules without bandwidth management.

## Using the Public Server Wizard

The SonicWALL **Public Server Wizard** provides an easy method for configuring firewall access rules for a SIP Proxy or H.323 Gatekeeper running on your network behind the firewall. Using this wizard performs all the configuration settings you need for VoIP clients to access your VoIP servers.

**Step 1** Click **Wizards** on the SonicOS navigation bar.

**Step 2** Select **Public Server Wizard** and click **Next**.



**Step 3** Select **Other** from the **Server Type** list.

- Select **SIP** from the **Services** menu if you're configuring network access for a SIP proxy server from the WAN.
- Select **Gatekeeper RAS** if you're configuring network access for a H.323 Gatekeeper from the WAN.
- Select **H.323 Call Signaling** for enabling Point-to-Point VoIP calls from the WAN to the LAN.

**Step 4** Click **Next**.



**Note**

SonicWALL recommends NOT selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.

**Step 2: Server Private Network Configuration**  
Enter the server's private (internal) address information.

Please enter a name to identify this server, and the server's private (internal) IP address. A Network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be renamed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

Server Name:

Server Private IP Address:

Server Comment:

To continue, click Next.

SONICWALL

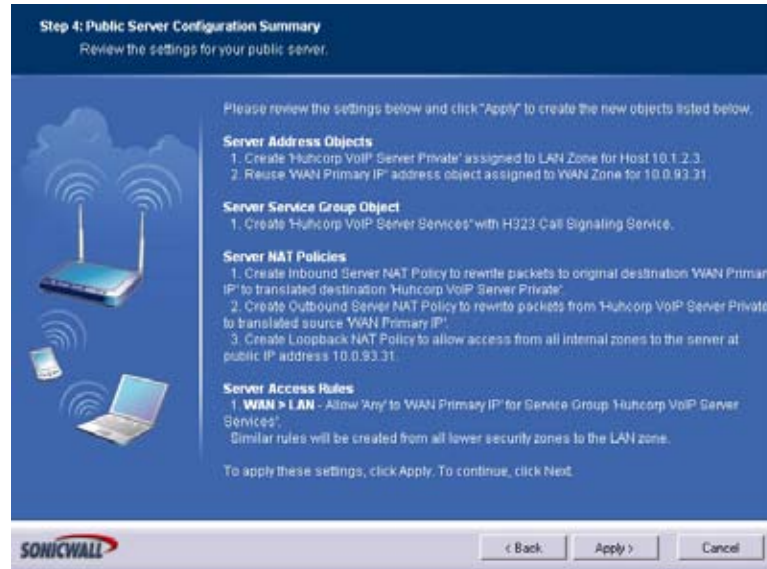
**Step 5** Enter the name of the server in the **Server Name** field.

**Step 6** Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to the zone where the server is located. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs. You can enter optional descriptive text in the Server Comment field.

**Step 7** Click **Next**.

**Step 8** Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

**Step 9** Click **Next**.



**Step 10** The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the LAN zone, the wizard binds the address object to the LAN zone.
- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server.
- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. The wizard also creates a Loopback NAT policy
- **Server Access Rules** - The wizard creates an access policy allowing all traffic to the WAN Primary IP for the new service.

**Step 11** Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWALL.



**Tip**

The new IP address used to access the new server, both internally and externally, is displayed in the **URL** field of the **Congratulations** window.

**Step 12** Click **Close** to close the wizard.

## Configuring VoIP Logging

You can enable the logging of VoIP events in the SonicWALL security appliance log in the **Log > Categories** page. Log entries are displayed on the **Log > View** page. To enable logging:

- 
- Step 1** Select **Log > Categories**.
  - Step 2** Select **Expanded Categories** from the **View Style** menu in the **Log Categories** section.
  - Step 3** Locate the **VoIP (VOIP H.323/RAS, H.323/H.225, H.323/H.245 activity)** entry in the table.
  - Step 4** Select **Log** to enable the display of VoIP log events in on the **Log > View** page.
  - Step 5** Select **Alerts** to enable the sending of alerts for the category.
  - Step 6** Select **Syslog** to enable the capture of the log events into the SonicWALL security appliance Syslog.
  - Step 7** Click **Apply**.

## VoIP Deployment Scenarios

SonicWALL security appliances can be deployed VoIP devices can be deployed in a variety of network configurations. This section describes the following deployment scenarios:

- “Generic Deployment Scenario” on page 531
- “Deployment Scenario 1: Point-to-Point VoIP Service” on page 531
- “Deployment Scenario 2: Public VoIP Service” on page 532
- “Deployment Scenario 3: Trusted VoIP Service” on page 533

### Generic Deployment Scenario

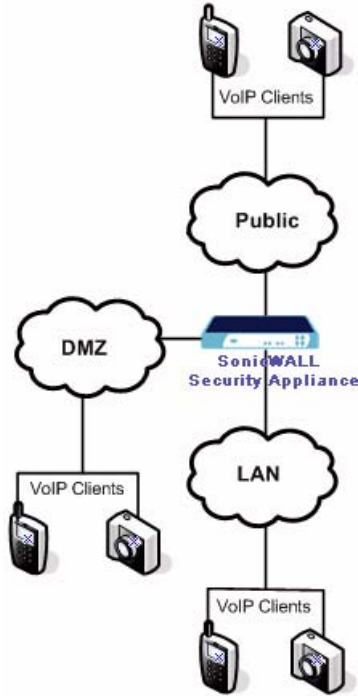
All three of the follow deployment scenarios begin with the following basic configuration procedure:

- 
- Step 1** Enable bandwidth management on the WAN interface on **Network > Interfaces**.
  - Step 2** Configure SIP or H.323 transformations and inactivity settings on **VoIP > Settings**.
  - Step 3** Configure the DHCP Server on the **Network > DHCP Server** page with static private IP address assignments to VoIP clients.
  - Step 4** Enable SonicWALL Intrusion Prevention Service to provided application-layer protection for VoIP communications on the **Security Services > Intrusion Prevention** page.
  - Step 5** Connect VoIP Clients to network.

### Deployment Scenario 1: Point-to-Point VoIP Service

The point-to-point VoIP service deployment is common for remote locations or small office environments that use a VoIP end point device connected to the network behind the firewall to receive calls directly from the WAN. The VoIP end point device on the Internet connects to VoIP client device on LAN behind the firewall using the SonicWALL security appliance’s Public IP address. The following figure shows a point-to-point VoIP service topology

**Figure 47:3 Point-to-Point VoIP Service Topology**



This deployment does not require a VoIP server. The Public IP address of the SonicWALL security appliance is used as the main VoIP number for hosts on the network. This requires a static Public IP address or the use of a Dynamic DNS service to make the public address available to callers from the WAN. Incoming call requests are routed through the SonicWALL security appliance using NAT, DHCP Server, and network access rules.

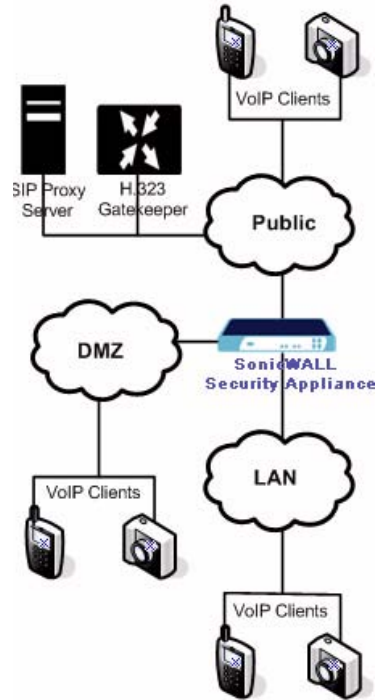
To make multiple devices behind the SonicWALL security appliance accessible from the public side, configure one-to-one NAT. If many-to-one NAT is configured, only one SIP and one NAT device will be accessible from the public side. See [“Network > NAT Policies” section on page 245](#) for more information on NAT.

See the [“Using the Public Server Wizard”](#) section for information on configuring this deployment.

## Deployment Scenario 2: Public VoIP Service

The Public VoIP Service deployment uses a VoIP service provider, which maintains the VoIP server (either a SIP Proxy Server or H.323 Gatekeeper). The SonicWALL security appliance public IP address provides the connection from the SIP Proxy Server or H.323 Gatekeeper operated by the VoIP service provider. The following figure shows a public VoIP service topology

**Figure 47:4 Public VoIP Service Topology**

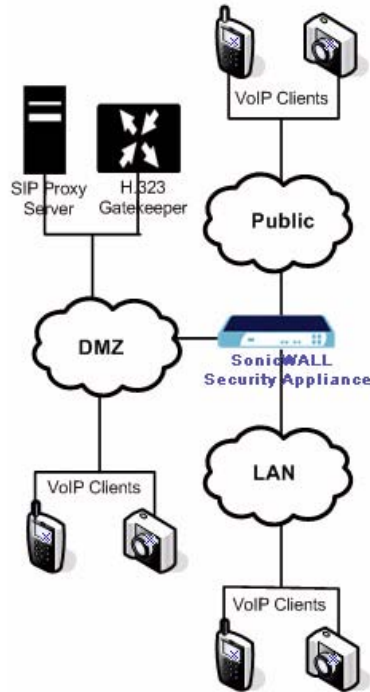


For VoIP clients that register with a server from the WAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration of clients is required. See the [“Using the Public Server Wizard”](#) section for information on configuring this deployment.

### Deployment Scenario 3: Trusted VoIP Service

The organization deploys its own VoIP server on a DMZ or LAN to provide in-house VoIP services that are accessible to VoIP clients on the Internet or from local network users behind the security gateway. The following figure shows a trusted VoIP service topology.

**Figure 47:5 Trusted VoIP Service Topology**



For VoIP clients that register with a server on the DMZ or LAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration on the VoIP clients is required.

To make a server on the LAN accessible to clients on the WAN:

7. Define a Host address object with the zone and IP address of the server.
8. Define a NAT policy, mapping traffic coming to the SonicWALL security appliance's public (WAN) IP address and VoIP service (SIP or H.323 Gatekeeper) to the server.
9. Define access rules allowing VoIP service to pass through the firewall.
10. See the "[Using the Public Server Wizard](#)" section for information on configuring this deployment.

# **PART 9**

# **VPN**





# CHAPTER 48

## Configuring VPN Policies

### VPN > Settings

The **VPN > Settings** page provides the SonicWALL features for configuring your VPN policies. You configure site-to-site VPN policies and GroupVPN policies from this page.

VPN > Settings

VPN Policy Wizard... Apply Cancel ?

VPN Global Settings

Enable VPN

Unique Firewall Identifier: 0006B111A2C4

VPN Policies

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Icons]
2	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	[Icons]
3	Wireless#2 GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Icons]
4	SonicWALL Site-2-Site	64.41.140.167	10.50.0.1 - 10.50.127.255 10.50.128.1 - 10.50.159.255	ESP 3DES HMAC MD5 (IKE)	<input checked="" type="checkbox"/>	[Icons]

Add... Delete... Delete All

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed

GroupVPN Policies: 3 Policies Defined, 1 Policies Enabled, 8 Maximum Policies Allowed

Currently Active VPN Tunnels

#	Name	Local	Remote	Gateway
No Entries				

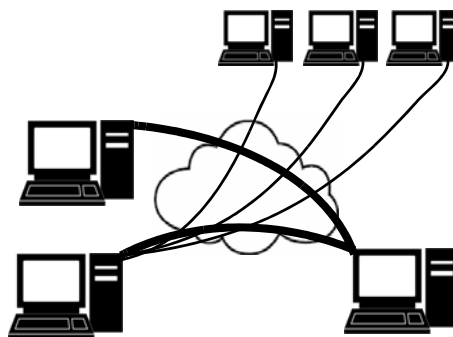
### VPN Overview

A Virtual Private Network (VPN) provides a secure connection between two or more computers or protected networks over the public internet. It provides authentication to ensure that the information is going to and from the correct parties. It provides security to protect the information from viewing or tampering en route.

Prior to the invention of Internet Protocol Security (IPsec) and Secure Socket Layer (SSL), secure connections between remote computers or networks required a dedicated line or satellite link. This was both inflexible and expensive.



A VPN creates a connection with similar reliability and security by establishing a secure tunnel through the internet. Because this tunnel is not a physical connection, it is more flexible--you can change it at any time to add more nodes, change the nodes, or remove it altogether. It is also far less costly, because it uses the existing internet infrastructure.



## VPN Types

There are two main types of VPN in popular use today:

- **IPsec VPN:** IPsec is a set of protocols for security at the packet processing layer of network communication. An advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. SonicOS supports the creation and management of IPsec VPNs.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header.

- **SSL VPN:** Secure Socket Layer (SSL) is a protocol for managing the security of a message transmission on the Internet, usually by HTTPS. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. An SSL VPN uses SSL to secure the VPN tunnel.

One advantage of SSL VPN is that SSL is built into most Web Browsers. No special VPN client software or hardware is required.



**Note**

SonicWALL makes SSL-VPN devices that you can use in concert with or independently of a SonicWALL UTM appliance running SonicOS. For information on SonicWALL SSL-VPN devices, see the SonicWALL Website :[http://www.sonicwall.com/us/Secure\\_Remote\\_Access.html](http://www.sonicwall.com/us/Secure_Remote_Access.html)

## VPN Security

IPsec VPN traffic is secured in two stages:

- **Authentication:** The first phase establishes the authenticity of the sender and receiver of the traffic using an exchange of the public key portion of a public-private key pair. This phase must be successful before the VPN tunnel can be established.
- **Encryption:** The traffic in the VPN tunnel is encrypted, using an encryption algorithm such as AES or 3DES.

Unless you use a manual key (which must be typed identically into each node in the VPN) The exchange of information to authenticate the members of the VPN and encrypt/decrypt the data uses the Internet Key Exchange (IKE) protocol for exchanging authentication information (keys) and establishing the VPN tunnel. SonicOS Enhanced supports two versions of IKE, version 1 and version 2.

### IKE version 1

IKE version 1 uses a two phase process to secure the VPN tunnel.

- **IKE Phase 1** is the authentication phase. The nodes or gateways on either end of the tunnel authenticate with each other, exchange encryption/decryption keys, and establish the secure tunnel.
- **IKE Phase 2** is the negotiation phase. Once authenticated, the two nodes or gateways negotiate the methods of encryption and data verification (using a hash function) to be used on the data passed through the VPN and negotiate the number of secure associations (SAs) in the tunnel and their lifetime before requiring renegotiation of the encryption/decryption keys.

#### IKE Phase 1

In IKE v1, there are two modes of exchanging authentication information: Main Mode and Aggressive Mode.

**Main Mode:** The node or gateway initiating the VPN queries the node or gateway on the receiving end, and they exchange authentication methods, public keys, and identity information. This usually requires six messages back and forth. The order of authentication messages in Main Mode is:

1. The initiator sends a list of cryptographic algorithms the initiator supports.
2. The responder replies with a list of supported cryptographic algorithms.
3. The initiator send a public key (part of a Diffie-Hellman public/private key pair) for the first mutually supported cryptographic algorithm.
4. The responder replies with the public key for the same cryptographic algorithm.
5. The initiator sends identity information (usually a certificate).
6. The responder replies with identity information.

**Aggressive Mode:** To reduce the number of messages exchanged during authentication by half, the negotiation of which cryptographic algorithm to use is eliminated. The initiator proposes one algorithm and the responder replies if it supports that algorithm:

1. The initiator proposes a cryptographic algorithms to use and sends its public key.
2. The responder replies with a public key and identity proof.
3. The initiator sends an identification proof. After authenticating, the VPN tunnel is established with two SAs, one from each node to the other.

### IKE Phase 2

In IKE phase 2, the two parties negotiate the type of security to use, which encryption methods to use for the traffic through the tunnel (if needed), and negotiate the lifetime of the tunnel before re-keying is needed.

The two types of security for individual packets are:

- **Encryption Secured Payload (ESP)**, in which the data portion of each packet is encrypted using a protocol negotiated between the parties.
- **Authentication Header (AH)**, in which the header of each packet contains authentication information to ensure the information is authentic and has not been tampered with. No encryption is used for the data with AH.

SonicOS supports the following encryption methods for Traffic through the VPN.

- DES
- 3DES
- AES-128
- AES-192
- AES-256



#### Note

You can find more information about IKE v1 in the three specifications that define initially define IKE, RFC 2407, RFC 2408, and RFC 2409, available on the web at:

<http://rfc.net/rfc2407.html>

<http://rfc.net/rfc2408.html>

<http://rfc.net/rfc2409.html>

## IKEv2

IKE version 2 is a new protocol for negotiating and establishing SAs. IKE v2 features improved security, a simplified architecture, and enhanced support for remote users. In addition, IKE v2 supports IP address allocation and EAP to enable different authentication methods and remote access scenarios. Using IKE V2 greatly reduces the number of message exchanges needed to establish an SA over IKE v1 Main Mode, while being more secure and flexible than IKE v1 Aggressive Mode. This reduces the delays during re-keying. As VPNS grow to include more and more tunnels between multiple nodes or gateways, IKE v2 reduces the number of SAs required per tunnel, thus reducing required bandwidth and housekeeping overhead.

IKE v2 is not compatible with IKE v1. If using IKE v2, all nodes in the VPN must use IKE v2 to establish the tunnels.

SAs in IKE v2 are called Child SAs and can be created, modified, and deleted independently at any time during the life of the VPN tunnel.

**Note**

There is no restriction on nesting IKE v1 tunnels within an IKE v2 tunnel and visa-versa. For example, if you are connecting to a wireless device using WiFiSec, which uses an IKE v1 tunnel, you can then connect over the internet to a corporate network using a site-to-site VPN tunnel established with IKE v2.

**Initialization and Authentication in IKE v2**

IKE v2 initializes a VPN tunnel with a pair of message exchanges (two message/response pairs).

- Initialize communication: The first pair of messages (IKE\_SA\_INIT) negotiate cryptographic algorithms, exchange nonces (random values generated and sent to guard against repeated messages), and perform a public key exchange.
  - a. Initiator sends a list of supported cryptographic algorithms, public keys, and a nonce.
  - b. Responder sends the selected cryptographic algorithm, the public key, a nonce, and an authentication request.
- Authenticate: The second pair of messages (IKE\_AUTH) authenticate the previous messages, exchange identities and certificates, and establish the first CHILD\_SA. Parts of these messages are encrypted and integrity protected with keys established through the IKE\_SA\_INIT exchange, so the identities are hidden from eavesdroppers and all fields in all the messages are authenticated.
  - a. Initiator identity proof, such as a shared secret or a certificate, and a request to establish a child SA.
  - b. Responder sends the matching identity proof and completes negotiation of a child SA.

**Negotiating SAs in IKE v2**

This exchange consists of a single request/response pair, and was referred to as a phase 2 exchange in IKE v1. It may be initiated by either end of the SA after the initial exchanges are completed.

All messages following the initial exchange are cryptographically protected using the cryptographic algorithms and keys negotiated in the first two messages of the IKE exchange.

Either endpoint may initiate a CREATE\_CHILD\_SA exchange, so in this section the term “initiator” refers to the endpoint initiating this exchange.

1. Initiator sends a child SA offer and, if the data is to be encrypted, the encryption method and the public key.
2. Responder sends the accepted child SA offer and, if encryption information was included, a public key.

**Note**

You can find more information about IKE v2 in the specification, RFC 4306, available on the web at:

<http://rfc.net/rfc4306.html>

For information on configuring VPNs in SonicOS Enhanced, see:

- “Configuring VPNs in SonicOS Enhanced” section on page 542
- “Configuring GroupVPN Policies” section on page 552
- “Site-to-Site VPN Configurations” section on page 561
- “Creating Site-to-Site VPN Policies” section on page 562

- [“VPN Auto-Added Access Rule Control” section on page 578](#)

## Configuring VPNs in SonicOS Enhanced

SonicWALL VPN, based on the industry-standard IPsec VPN implementation, provides a easy-to-setup, secure solution for connecting mobile users, telecommuters, remote offices and partners via the Internet. Mobile users, telecommuters, and other remote users with broadband (DSL or cable) or dialup Internet access can securely and easily access your network resources with the SonicWALL Global VPN Client or Global Security Client and SonicWALL GroupVPN on your SonicWALL. Remote office networks can securely connect to your network using site-to-site VPN connections that enable network-to- network VPN connections.



### Note

For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator’s Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator’s Guide**.

SonicWALL’s GroupVPN provides automatic VPN policy provisioning for SonicWALL Global VPN Clients. The GroupVPN feature on the SonicWALL security appliance and the SonicWALL Global VPN Client (part of the Global security Client) dramatically streamline VPN deployment and management. Using SonicWALL’s Client Policy Provisioning technology, you define the VPN policies for Global VPN Client users. This policy information automatically downloads from the SonicWALL security appliance (VPN Gateway) to Global VPN Clients, saving remote users the burden of provisioning VPN connections.

You can easily and quickly create a site-to-site VPN policy or a GroupVPN policy for SonicWALL Global Security Clients using the **VPN Policy Wizard**. You can also configure GroupVPN or site-to-site VPN tunnels using the Management Interface. You can define up to four GroupVPN policies, one for each Zone. You can also create multiple site-to-site VPN. The maximum number of policies you can add depends on your SonicWALL model.

## Planning Your VPN

Before creating or activating a VPN tunnel, gather the following information. You can print these pages and to use as a planning checklist:

### GroupVPN Policy Planning Checklist

#### On the SonicWALL security appliance:

- **Authentication Method:**
    - IKE using Preshared Secret
    - IKE using 3rd Party Certificates.
  - **Shared Secret** if using preshared secret.
- 
- **Gateway Certificate** if using 3rd part certificates. This is a certificate file you have uploaded to your SonicWALL security appliance and plan to distribute to your VPN Clients.
- 
- **Peer ID Type** if using 3rd party certificates: Choose
    - Distinguished Name

- E-Mail ID
- Domain name.
- **Peer ID Filter** if using 3rd party certificates.

---

- **IKE (Phase 1) Proposal:**

- **DH Group:**
- Group 1
- Group 2
- Group 5

**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

---

- **Encryption:**
- DES
- 3DES
- AES-128
- AES-256
- **Authentication:**
- MD5
- SHA1
- **Life Time** (seconds): \_\_\_\_\_ (default 28800)

- **Ipssec (Phase 2) Proposal:**

- **Protocol:** (ESP only)
- **Encryption:**
- DES
- 3DES
- AES-128
- AES-192
- **AES-256**
- **Authentication:**
- MD5
- SHA1
- **Enable Perfect Forward Secrecy**
- **DH Group** (if perfect forward secrecy is enabled):
- Group 1
- Group 2
- Group 5

**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- **Life Time** (seconds): \_\_\_\_\_ (default 28800)
- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Management via this SA:**
  - HTTP**
  - HTTPS**
- **Default Gateway:**
- **Enable OCSP Checking**
  - **OCSP Responder URL:** \_\_\_\_\_
- **Require Authentication of VPN Clients via XAUTH**
- **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):  
\_\_\_\_\_
- **Allow Unauthenticated VPN Client Access** (the network or subnet you will allow to have access to this VPN without authentication if XAUTH is not selected):  
\_\_\_\_\_
- **Cache XAUTH User Name and Password on Client** (will the client be able to store the user name and password):
  - Never**
  - Single Session**
  - Always**
- **Virtual Adapter settings:**
  - None**
  - DHCP Lease**
  - DHCP Lease or Manual Configuration**
- **Allow Connections to:**
  - This Gateway Only**
  - All Secured Gateways**
  - Split Tunnels**
- **Set Default Route as this Gateway**
- **Require Global Security Client for this Connection**
- **Use Default Key for Simple Client Provisioning**  
(this allows easier client setup, but is less secure)

**On the client**

- IP address or Web address of VPN Gateway
- VPN Client:
  - GVC or GSC**



- GSC only (Require Global Security Client checked on security appliance)
- Shared secret, if selected on security appliance:
  - \_\_\_\_\_
- Certificate, if selected on security appliance:
  - \_\_\_\_\_
- User's user name and password if XAUTH is required on the security appliance.

## Site-to-Site VPN Planning Checklist

### On the Initiator

Typically, the request for an IKE VPN SA is made from the remote site.

- **Authentication Method:**
  - Manual Key
  - IKE using Preshared Secret
  - IKE using 3rd Party Certificates (not used with IKEv2)
- **Name of this VPN:** \_\_\_\_\_
- **IPsec Primary Gateway Name or Address:**
  - \_\_\_\_\_
- **IPsec Secondary Gateway Name or Address:**
  - \_\_\_\_\_
  - (not used with manual key, not used with IKEv2)
- **IKE Authentication for IKE using Preshared Secret:**
  - **Shared Secret:** \_\_\_\_\_
  - **Local IKE ID:**
    - IP Address \_\_\_\_\_
    - Domain Name \_\_\_\_\_
    - Email Address \_\_\_\_\_
    - SonicWALL Identifier \_\_\_\_\_
  - **Peer IKE ID:**
    - IP Address \_\_\_\_\_
    - Domain Name \_\_\_\_\_
    - Email Address \_\_\_\_\_
    - SonicWALL Identifier \_\_\_\_\_
- **IKE Authentication for IKE using 3rd Party Certificate (not used with IKEv2):**
  - **Local Certificate:** \_\_\_\_\_
  - **Peer IKE ID Type:**
    - Distinguished name
    - E-Mail ID
    - Domain name
  - **Peer IKE ID:** \_\_\_\_\_
- **Local Networks**

— Choose local network from list (select an address object):

Local network obtains IP addresses using DHCP through this VPN Tunnel  
(not used with IKEv2)

Any address

• Destination Networks

Use this VPN Tunnel as default route for all Internet traffic

Destination network obtains IP addresses using DHCP through this VPN Tunnel

Choose destination network from list (select an address object):

• IKE (Phase 1) Proposal:

– Exchange:

–  Main Mode

–  Aggressive Mode

–  IKEv2 Mode

– DH Group:

–  Group 1

–  Group 2

–  Group 5



**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

– Encryption:

–  DES

–  3DES

–  AES-128

–  AES-192

–  **AES-256**

– Authentication:

–  MD5

–  SHA1

– Life Time (seconds): \_\_\_\_\_ (default 28800)

• Ipsec (Phase 2) Proposal

– Protocol:

–  ESP

–  AH

– Encryption:

–  DES

–  3DES

–  AES-128

- AES-192
- AES-256
- Authentication:
  - MD5
  - SHA1
  - **Enable Perfect Forward Secrecy**
  - **DH Group** (if perfect forward secrecy is enabled):
    - Group 1
    - Group 2
    - Group 5

**Note**

The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- **Life Time** (seconds): \_\_\_\_\_ (default 28800)
- **Enable Keep Alive**
- **Suppress automatic Access Rules creation for VPN Policy**
- **Require authentication of VPN clients by XAUTH** (not with IKEv2)
  - **User Group for XAUTH users** (the user group that will have access to this VPN if XAUTH is selected):  
\_\_\_\_\_
- **Enable Windows Networking (NetBIOS) Broadcast**
- **Enable Multicast**
- **Apply NAT Policies**
  - **Translated Local Network:** \_\_\_\_\_
  - **Translated Remote Network:** \_\_\_\_\_
- **Enable OCSP Checking** (IKE with 3rd Party Certificate only)
  - **OCSP Responder URL:** (IKE with 3rd Party Certificate only)  
\_\_\_\_\_
- **Management via this SA:**
  - HTTP
  - HTTPS
- **User login via this SA:**
  - HTTP
  - HTTPS
- **Default LAN Gateway (optional):**
- **VPN Policy bound to:**
  - Zone WAN
- **Do not send trigger packet during IKE SA negotiation** (IKEv2 only)

**On the Responder**

The settings on the responder must be the same as on the initiator except:

- **Name** of this VPN: \_\_\_\_\_
- **IPsec Primary Gateway Name or Address**: not required on the responder
- **IPsec Secondary Gateway Name or Address**: not required on the responder
- **IKE Authentication for IKE using Preshared Secret**:
  - **Local IKE ID**: (must match Peer IKE ID on initiator)
  - **IP Address** \_\_\_\_\_
  - **Domain Name** \_\_\_\_\_
  - **Email Address** \_\_\_\_\_
  - **SonicWALL Identifier** \_\_\_\_\_
  - **Peer IKE ID**: (must match Local IKE ID on initiator)
  - **IP Address** \_\_\_\_\_
  - **Domain Name** \_\_\_\_\_
  - **Email Address** \_\_\_\_\_
  - **SonicWALL Identifier** \_\_\_\_\_
- **IKE Authentication for IKE using 3rd Party Certificate** (not used with IKEv2):
  - **Local Certificate**: \_\_\_\_\_
  - **Peer IKE ID Type**:
    - Distinguished name
    - E-Mail ID
    - Domain name
  - **Peer IKE ID**: \_\_\_\_\_
- **Local Networks** (must match Destination Networks on initiator)
  - Choose local network from list** (select an address object):  
\_\_\_\_\_
  - Local network obtains IP addresses using DHCP through this VPN Tunnel**  
(not used with IKEv2)
  - Any address**
- **Destination Networks** (must match Local Networks on initiator)
  - Use this VPN Tunnel as default route for all Internet traffic**
  - Destination network obtains IP addresses using DHCP through this VPN Tunnel**
  - Choose destination network from list** (select an address object):  
\_\_\_\_\_
- **Apply NAT Policies**
  - **Translated Local Network**: (must match Translated Remote Network on initiator)  
\_\_\_\_\_
  - **Translated Remote Network** (must match Translated Local Network on initiator)  
\_\_\_\_\_

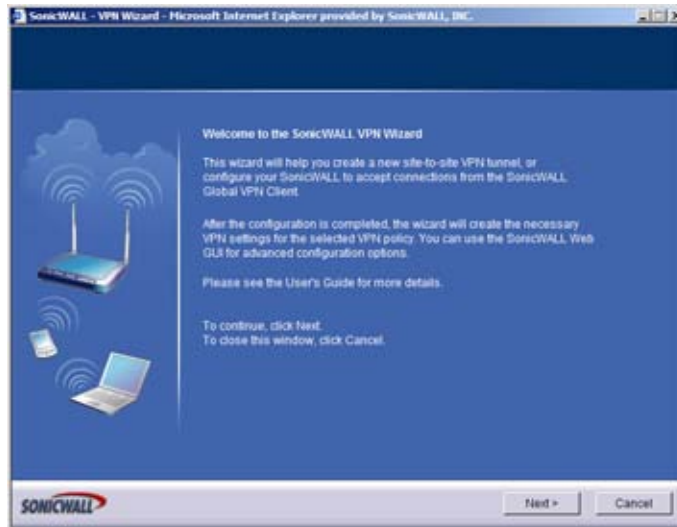
## VPN Policy Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN or site-to-site VPN policies on the SonicWALL security appliance. After completing the configuration, the wizard creates the necessary VPN settings for the selected policy. You can use the SonicWALL Management Interface for optional advanced configuration options.



**Note**

For step-by-step instructions on using the VPN Policy Wizard, see Chapter 50 Configuring VPNs with the VPN Policy Wizard.



## VPN Global Settings

The **Global VPN Settings** section of the **VPN > Settings** page displays the following information:



- **Enable VPN** must be selected to allow VPN policies through the SonicWALL security policies.
- **Unique Firewall Identifier** - the default value is the serial number of the SonicWALL. You can change the Identifier, and use it for configuring VPN tunnels.

## VPN Policies

All existing VPN policies are displayed in the **VPN Policies** table. Each entry displays the following information:

Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Edit] [Trash] [Disk]
2 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	[Edit] [Trash] [Disk]
3 Wireless#2 GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	[Edit] [Trash] [Disk]
4 SonicWALL Site-2-Site	199.55.155.155	10.10.0.1 - 10.10.127.255 10.10.128.1 - 10.10.159.255	ESP 3DES HMAC MD5 (IKE)	<input checked="" type="checkbox"/>	[Edit] [Trash] [Disk]

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 50 Maximum Policies Allowed  
GroupVPN Policies: 3 Policies Defined, 1 Policies Enabled, 8 Maximum Policies Allowed

- **Name:** Displays the default name or user-defined VPN policy name.
- **Gateway:** Displays the IP address of the remote SonicWALL. If 0.0.0.0 is used, no Gateway is displayed.
- **Destinations:** Displays the IP addresses of the destination networks.
- **Crypto Suite:** Displays the type of encryption used for the VPN policy.
- **Enable:** Selecting the check box enables the VPN Policy. Clearing the check box disables it.
- **Configure:** Clicking the Edit icon allows you to edit the VPN policy. Clicking the Trashcan allows you to delete the VPN policy. The predefined GroupVPN policies cannot be deleted, so the Trashcan icons are dimmed. GroupVPN policies also have a Disk icon for exporting the VPN policy configuration as a file for local installation by SonicWALL Global VPN Clients.

The number of VPN policies defined, policies enabled, and the maximum number of Policies allowed is displayed below the table. You can define up to 4 GroupVPN policies, one for each Zone. These GroupVPN policies are listed by default in the VPN Policies table as **WAN GroupVPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. Clicking on the edit icon in the Configure column for the GroupVPN displays the **VPN Policy** window for configuring the GroupVPN policy.

Below the VPN Policies table are the following buttons:

- **Add** - Accesses the **VPN Policy** window to configure site-to-site VPN policies.
- **Delete** - Deletes the selected (checked box before the VPN policy name in the **Name** column. You cannot delete the GroupVPN policies.
- **Delete All** - Deletes all VPN policies in the VPN Policies table except the default GroupVPN policies.

### Navigating and Sorting the VPN Policies Entries

The **VPN Policies** table provides easy pagination for viewing a large number of VPN policies. You can navigate a large number of VPN policies listed in the **VPN Policies** table by using the navigation control bar located at the top right of the **VPN Policies** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can enter the policy number (the number listed before the policy name in the **# Name** column) in the **Items** field to move to a specific VPN policy. The default table configuration displays 50 entries per page. You can change this default number of entries for tables on the **System > Administration** page.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.


## Currently Active VPN Tunnels

A list of currently active VPN tunnels is displayed in this section. The table lists the name of the VPN Policy, the local LAN IP addresses, and the remote destination network IP addresses as well as the peer gateway IP address.

#	Name	Local	Remote	Gateway
1	WLAN GroupVPN	0.0.0.1-255.255.255.255	fcheck	172.16.31.233

Click the **Renegotiate** button to force the VPN Client to renegotiate the VPN tunnel.

## Viewing VPN Tunnel Statistics

In the Currently Active VPN Tunnels table, click on the Statistics icon  in the row for a tunnel to view the statistics on that tunnel. The VPN Tunnel Statistics icon displays:

Description	Value
Create Time	02/02/2006 19:16:40
Tunnel valid until	02/03/2006 03:16:40
Packets In	23
Packets Out	7
Bytes In	1894
Bytes Out	2957
Fragmented Packets In	0
Fragmented Packets Out	0

- **Create Time:** The date and time the tunnel came into existence.
- **Tunnel valid until:** The time when the tunnel expires and is force to renegotiate.
- **Packets In:** The number of packets received from this tunnel.
- **Packets Out:** The number of packets sent out from this tunnel.
- **Bytes In:** The number of bytes received from this tunnel.
- **Bytes Out:** The number of bytes sent out from this tunnel.
- **Fragmented Packets In:** The number of fragmented packets received from this tunnel.
- **Fragmented Packets Out:** The number of fragmented packets sent out from this tunnel.

For detailed information on configuring VPNs in SonicOS Enhanced, see:

- [“Configuring GroupVPN Policies” section on page 552](#)
- [“Site-to-Site VPN Configurations” section on page 561](#)

- “Creating Site-to-Site VPN Policies” section on page 562
- “VPN Auto-Added Access Rule Control” section on page 578

## Configuring GroupVPN Policies

SonicWALL **GroupVPN** facilitates the set up and deployment of multiple SonicWALL Global VPN Clients by the SonicWALL security appliance administrator. **GroupVPN** is only available for SonicWALL Global VPN Clients and it is recommended you use XAUTH/RADIUS or third party certificates in conjunction with the **Group VPN** for added security.

For more information on the SonicWALL Global VPN Client, see the **SonicWALL Global VPN Client Administrator’s Guide**. For more information on the SonicWALL Global Security Client, see the **SonicWALL Global Security Client Administrator’s Guide**.

The default GroupVPN configuration allows you to support SonicWALL Global VPN Clients without any further editing of the VPN policy, except to check the **Enable** box for GroupVPN in the **VPN Policies** table.

SonicWALL supports four GroupVPN policies. You can create GroupVPN policies for the DMZ, LAN, WAN, and WLAN zones. These GroupVPN policies are listed in the VPN policies tables as **WAN Group VPN**, **LAN GroupVPN**, **DMZ GroupVPN**, and **WLAN GroupVPN**. For these GroupVPN policies, you can choose from **IKE using Preshared Secret** or **IKE using 3rd Party Certificates** for your IPsec Keying Mode.



### Tip

---

You can easily create GroupVPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNs with the SonicWALL VPN Policy Wizard.

---



### Note

---

See the **GroupVPN Setup in SonicOS Enhanced** technote on the SonicWALL documentation Web site <http://www.sonicwall.com> for more GroupVPN configuration information.

---

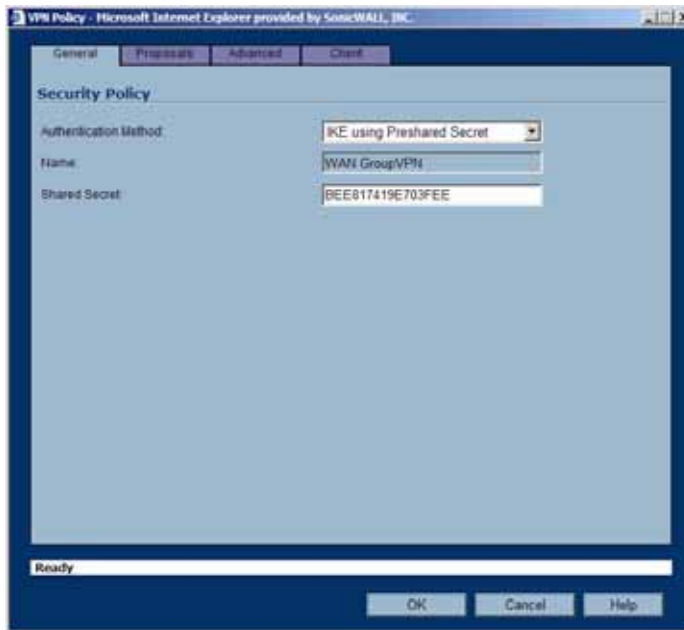
SonicOS supports the creation and management of IPsec VPNs.



## Configuring GroupVPN with IKE using Preshared Secret on the WAN Zone

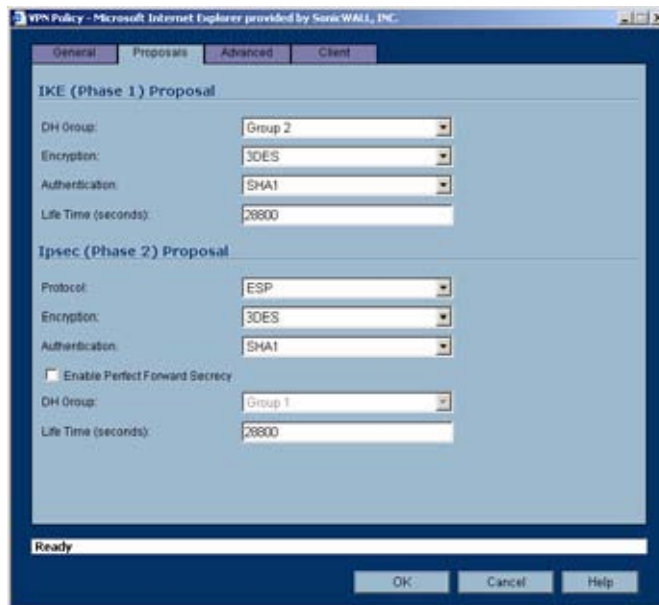
To configure the WAN GroupVPN, follow these steps:

- Step 1** Click the **edit** icon for the **WAN GroupVPN** entry. The **VPN Policy** window is displayed.



- Step 2** In the **General** tab, **IKE using Preshared Secret** is the default setting for **Authentication Method**. A Shared Secret is automatically generated by the SonicWALL security appliance in the **Shared Secret** field, or you can generate your own shared secret. **Shared Secrets** must be minimum of four characters. You cannot change the name of any GroupVPN policy.

- Step 3** Click the **Proposals** tab to continue the configuration process.



- Step 4** In the **IKE (Phase 1) Proposal** section, use the following settings:

- Select the DH Group from the **DH Group** menu.



**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

**Step 5** In the **IPsec (Phase 2) Proposal** section, select the following settings:

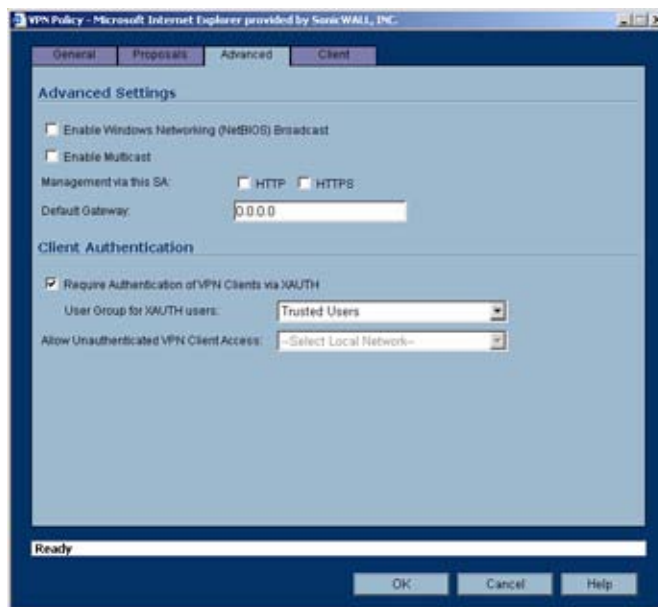
- Select the desired protocol from the **Protocol** menu.
- Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

**Step 6** Click the **Advanced** tab.

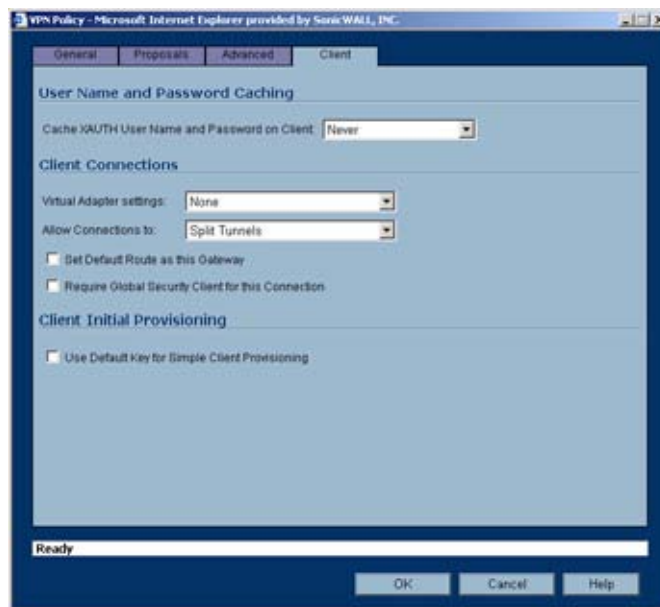


**Step 7** Select any of the following optional settings you want to apply to your GroupVPN policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows® Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.

- **Management via this SA:** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Allows the network administrator to specify the IP address of the default network route for incoming IPsec packets for this VPN policy. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL security appliance. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the traffic. For packets received via an IPsec tunnel, the SonicWALL looks up a route. If no route is found, the security appliance checks for a Default Gateway. If a Default Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN tunnel is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel. The **Trusted users** group is selected by default. You can select another user group or **Everyone** from **User Group for XAUTH users**.
- **Allow Unauthenticated VPN Client Access** - Allows you to enable unauthenticated VPN client access. If you uncheck **Require Authentication of VPN Clients via XAUTH**, the **Allow Unauthenticated VPN Client Access** menu is activated. Select an Address Object or Address Group from menu of predefined options, or select **Create new address object** or **Create new address group** to create a new one.

**Step 8** Click the **Client** tab, select any of the following settings you want to apply to your GroupVPN policy.



- **Cache XAUTH User Name and Password on Client** - Allows the Global VPN Client to cache the user name and password.
  - **Never** - Global VPN Client is not allowed to cache the username and password. The user will be prompted for a username and password when the connection is enabled, and also every time there is an IKE Phase 1 rekey.
  - **Single Session** - Global VPN Client user prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. The username and password is used through IKE Phase 1 rekey.

- **Always** - Global VPN Client user prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it's necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
- **None** - A Virtual Adapter will not be used by this GroupVPN connection.
- **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
- **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.
- **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
- **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this VPN tunnel. You can only configure one VPN policy to use this setting.
- **Require Global Security Client for this Connection** - Only allows a VPN connection from a remote computer running the SonicWALL Global Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

**Note**

For more information on the SonicWALL Global Security Client, see the SonicWALL Global Security Client Administrator's Guide.

- **Use Default Key for Simple Client Provisioning** - uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

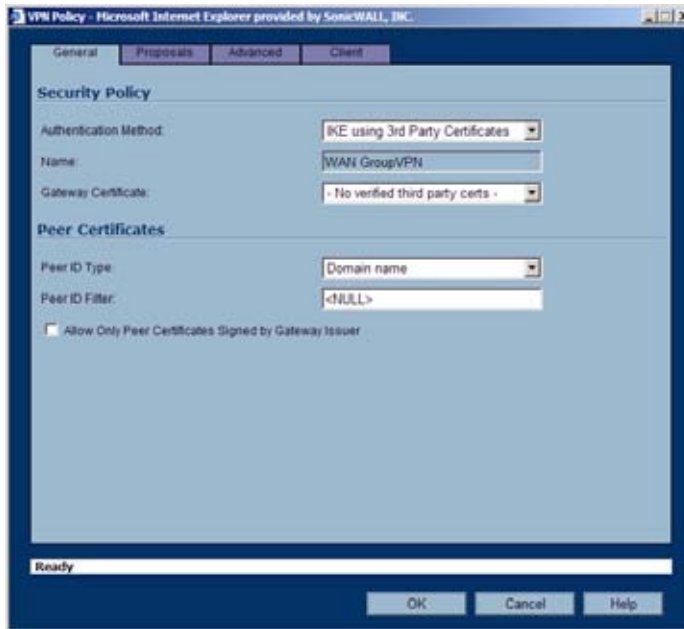
**Step 9** Click **OK**.

## Configuring GroupVPN with IKE using 3rd Party Certificates

To configure GroupVPN with IKE using 3rd Party Certificates, follow these steps:

**Caution** Before configuring GroupVPN with IKE using 3rd Party Certificates, your certificates must be installed on the SonicWALL.

**Step 1** In the **VPN > Settings** page click the edit icon under **Configure**. The **VPN Policy** window is displayed.



**Step 2** In the **Security Policy** section, select **IKE using 3rd Party Certificates** from the **Authentication Method** menu. The VPN policy name is **GroupVPN** by default and cannot be changed.

**Step 3** Select a certificate for the SonicWALL from the **Gateway Certificate** menu.

**Step 4** Select one of the following Peer ID types from the **Peer ID Type** menu:

- **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters \* (for more than 1 character) and ? (for a single character). For example, the string \*@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string \*sv.us.sonicwall.com when **Domain Name** is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.

- **Distinguished Name** - based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=). Up to three organizational units can be specified. The usage is c=\*;o=\*;ou=\*;ou=\*;ou=\*;cn=\*. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. c=us.

**Step 5** Enter the Peer ID filter in the **Peer ID Filter** field.

**Step 6** Check **Allow Only Peer Certificates Signed by Gateway Issuer** to specify that peer certificates must be signed by the issuer specified in the **Gateway Certificate** menu.

**Step 7** Click on the **Proposals** tab.

**Step 8** In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select the DH Group from the **DH Group** menu.



**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

**Step 9** In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES, AES-128, or AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.



**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

**Step 10** Click on the **Advanced** tab and select any of the following optional settings that you want to apply to your GroupVPN Policy:

- **Enable Windows Networking (NetBIOS) broadcast** - Allows access to remote network resources by browsing the Windows Network Neighborhood.
- **Enable Multicast** - Enables IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- **Management via this SA** - If using the VPN policy to manage the SonicWALL security appliance, select the management method, either **HTTP** or **HTTPS**.
- **Default Gateway** - Used at a central site in conjunction with a remote site using the **Route all Internet traffic through this SA** check box. Default LAN Gateway allows the network administrator to specify the IP address of the default LAN route for incoming IPsec packets for this SA. Incoming packets are decoded by the SonicWALL and compared to static routes configured in the SonicWALL. Since packets can have any IP address destination, it is impossible to configure enough static routes to handle the

traffic. For packets received via an IPsec tunnel, the SonicWALL looks up a route for the LAN. If no route is found, the SonicWALL checks for a Default LAN Gateway. If a Default LAN Gateway is detected, the packet is routed through the gateway. Otherwise, the packet is dropped.

- **Enable OCSP Checking** and **OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See the [“Using OCSP with SonicWALL Security Appliances”](#) section in the [“VPN > Settings”](#) section on page 537.
- **Require Authentication of VPN Clients via XAUTH** - Requires that all inbound traffic on this VPN policy is from an authenticated user. Unauthenticated traffic is not allowed on the VPN tunnel.
- **User group for XAUTH users** - Allows you to select a defined user group for authentication.
- **All Unauthenticated VPN Client Access** - Allows you to specify network segments for unauthenticated Global VPN Client access.

**Step 11** Click on the **Client** tab and select any of the following boxes that you want to apply to Global VPN Client provisioning:

- **Cache XAUTH User Name and Password** - Allows the Global VPN Client to cache the user name and password. Select from:
  - **Never** - Global VPN Client is not allowed to cache username and password. The user will be prompted for a username and password when the connection is enabled and also every time there is an IKE phase 1 rekey.
  - **Single Session** - The user will be prompted for username and password each time the connection is enabled and will be valid until the connection is disabled. This username and password is used through IKE phase 1 rekey.
  - **Always** - The user will be prompted for username and password only once when connection is enabled. When prompted, the user will be given the option of caching the username and password.
- **Virtual Adapter Settings** - The use of the Virtual Adapter by the Global VPN Client (GVC) is dependent upon a DHCP server, either the internal SonicOS or a specified external DHCP server, to allocate addresses to the Virtual Adapter. In instances where predictable addressing was a requirement, it's necessary to obtain the MAC address of the Virtual Adapter, and to create a DHCP lease reservation. To reduce the administrative burden of providing predictable Virtual Adapter addressing, you can configure the GroupVPN to accept static addressing of the Virtual Adapter's IP configuration. This feature requires the use of GVC version 3.0 or later.
  - **None** - A Virtual Adapter will not be used by this GroupVPN connection.
  - **DHCP Lease** - The Virtual Adapter will obtain its IP configuration from the DHCP Server only, as configure in the **VPN > DHCP over VPN** page.
  - **DHCP Lease or Manual Configuration** - When the GVC connects to the SonicWALL, the policy from the SonicWALL instructs the GVC to use a Virtual Adapter, but the DHCP messages are suppressed if the Virtual Adapter has been manually configured. The configured value is recorded by the SonicWALL so that it can proxy ARP for the manually assigned IP address. By design, there are currently no limitations on IP address assignments for the Virtual Adapter. Only duplicate static addresses are not permitted.
- **Allow Connections to** - Client network traffic matching destination networks of each gateway is sent through the VPN tunnel of that specific gateway.

- **This Gateway Only** - Allows a single connection to be enabled at a time. Traffic that matches the destination networks as specified in the policy of the gateway is sent through the VPN tunnel. If this option is selected along with Set Default Route as this Gateway, then the Internet traffic is also sent through the VPN tunnel. If this option is selected without selecting Set Default Route as this Gateway, then the Internet traffic is blocked.
- **All Secured Gateways** - Allows one or more connections to be enabled at the same time. Traffic matching the destination networks of each gateway is sent through the VPN tunnel of that specific gateway. If this option is selected along with **Set Default Route as this Gateway**, then Internet traffic is also sent through the VPN tunnel. If this option is selected without **Set Default Route as this Gateway**, then the Internet traffic is blocked. Only one of the multiple gateways can have **Set Default Route as this Gateway** enabled.
- **Split Tunnels** - Allows the VPN user to have both local Internet connectivity and VPN connectivity.
- **Set Default Route as this Gateway** - Enable this check box if all remote VPN connections access the Internet through this SA. You can only configure one SA to use this setting.
- **Require Global Security Client for this Connection** - Only allows a VPN connection from a remote computer running the SonicWALL Global Security Client, which provides policy enforced firewall protection before allowing a Global VPN Client connection.

**Note**

---

For more information on the SonicWALL Global Security Client and Distributed Security Client, see the SonicWALL Global Security Client Administrator's Guide.

---

- **Use Default Key for Simple Client Provisioning** - Uses Aggressive mode for the initial exchange with the gateway and VPN clients uses a default Preshared Key for authentication.

**Step 12** Click **OK**.

## Exporting a VPN Client Policy

If you want to export the Global VPN Client configuration settings to a file for users to import into their Global VPN Clients, follow these instructions:



**Caution** The GroupVPN SA must be enabled on the SonicWALL to export a configuration file.

**Step 1** Click the **Disk** icon in the **Configure** column for the GroupVPN entry in the **VPN Policies** table. The **Export VPN Client Policy** window appears.



**Step 2** **rcf format is required for SonicWALL Global VPN Clients** is selected by default. Files saved in the rcf format can be password encrypted. The SonicWALL provides a default file name for the configuration file, which you can change.

**Step 3** Click **Yes**. The **VPN Policy Export** window appears.

**Step 4** Type a password in the **Password** field and reenter it in the **Confirm Password** field, if you want to encrypt the exported file. If you choose not to enter a password, the exported file is not encrypted.

**Step 5** Click **Submit**. If you did not enter a password, a message appears confirming your choice.

**Step 6** Click **OK**. You can change the configuration file before saving.

**Step 7** Save the file.

**Step 8** Click **Close**.

The file can be saved to a floppy disk or sent electronically to remote users to configure their Global VPN Clients.

## Site-to-Site VPN Configurations

When designing VPN connections, be sure to document all pertinent IP Addressing information and create a network diagram to use as a reference. A sample planning sheet is provided on the next page. The SonicWALL must have a routable WAN IP Address whether it is dynamic or static. In a VPN network with dynamic and static IP addresses, the VPN gateway with the dynamic address must initiate the VPN connection.

Site-to-Site VPN configurations can include the following options:

- **Branch Office (Gateway to Gateway)** - A SonicWALL is configured to connect to another SonicWALL via a VPN tunnel. Or, a SonicWALL is configured to connect via IPsec to another manufacturer's firewall.

- **Hub and Spoke Design** - All SonicWALL VPN gateways are configured to connect to a central SonicWALL (hub), such as a corporate SonicWALL. The hub must have a static IP address, but the spokes can have dynamic IP addresses. If the spokes are dynamic, the hub must be a SonicWALL.
- **Mesh Design** - All sites connect to all other sites. All sites must have static IP addresses. See “Planning Your VPN” on page 542 for a planning sheet to help you set up your VPN.

## Creating Site-to-Site VPN Policies



### Tip

---

You can easily create site-to-site VPN policies using the VPN Policy Wizard. For complete step-by-step instructions on using the VPN Policy Wizard, see Chapter 51 Configuring VPNs with the SonicWALL VPN Policy Wizard.

---

You can create or modify existing VPN policies using the VPN Policy window. Clicking the **Add** button under the **VPN Policies** table displays the **VPN Policy** window for configuring the following IPsec Keying mode VPN policies:

- IKE using Preshared Key
- Manual Key
- IKE using 3rd Party Certificates



### Tip

---

Use the VPN Planning Sheet for Site-to-Site VPN Policies to record your settings. These settings are necessary to configure the remote SonicWALL and create a successful VPN connection.

---



### Note

---

For configuring VPN policies between SonicWALL security appliances running SonicOS Enhanced and SonicWALL security appliances running SonicWALL Firmware version 6.5 (or higher), see the technote: Creating IKE IPsec VPN Tunnels between SonicWALL Firmware 6.5 and SonicOS Enhanced, available at the SonicWALL documentation Web site <http://www.sonicwall.com/us/Support.html>.

---

## Configuring a VPN Policy with IKE using Preshared Secret

To configure a VPN Policy using Internet Key Exchange (IKE), follow the steps below:

- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.

- Step 2** In the **General** tab, select **IKE using Preshared Secret** from the **Authentication Method** menu.
- Step 3** Enter a name for the policy in the **Name** field.
- Step 4** Enter the host name or IP address of the remote connection in the **IPsec Primary Gateway Name or Address** field.
- Step 5** If the Remote VPN device supports more than one endpoint, you may optionally enter a second host name or IP address of the remote connection in the **IPsec Secondary Gateway Name or Address** field.

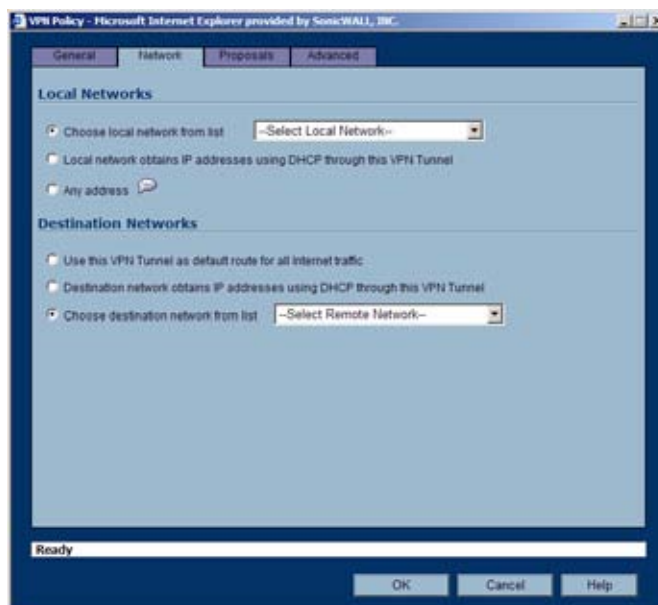


**Note** Secondary gateways are not supported with IKEv2.

- Step 6** Enter a Shared Secret password to be used to setup the Security Association the **Shared Secret** and **Confirm Shared Secret** fields. The Shared Secret must be at least 4 characters long, and should comprise both numbers and letters.

Optionally, specify a **Local IKE ID (optional)** and **Peer IKE ID (optional)** for this Policy. By default, the **IP Address (ID\_IPv4\_ADDR)** is used for Main Mode negotiations, and the SonicWALL Identifier (**ID\_USER\_FQDN**) is used for Aggressive Mode.

**Step 7** Click the **Network** tab.



**Step 8** Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN tunnel as default route for all Internet traffic** selected.

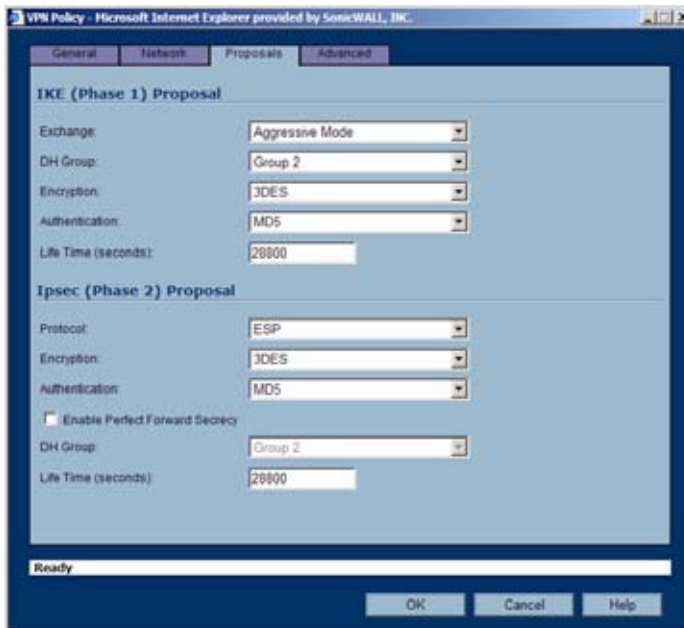


**Note** DHCP over VPN is not supported with IKEv2.

**Step 9** Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select

**Destination network obtains IP addresses using DHCP server through this tunnel.** Alternatively, select **Choose Destination network from list**, and select the address object or group.

**Step 10** Click **Proposals**.



**Step 11** Under **IKE (Phase 1) Proposal**, select either **Main Mode**, **Aggressive Mode**, or **IKEv2** from the **Exchange** menu. **Aggressive Mode** is generally used when WAN addressing is dynamically assigned. **IKEv2** causes all the negotiation to happen via IKE v2 protocols, rather than using IKE Phase 1 and Phase 2. If you use IKE v2, both ends of the VPN tunnel must use IKE v2.

**Step 12** Under **IKE (Phase 1) Proposal**, the default values for **DH Group**, **Encryption**, **Authentication**, and **Life Time** are acceptable for most VPN configurations. Be sure the Phase 1 values on the opposite side of the tunnel are configured to match. You can also choose **AES-128**, **AES-192**, or **AES-256** from the **Authentication** menu instead of 3DES for enhanced authentication security.

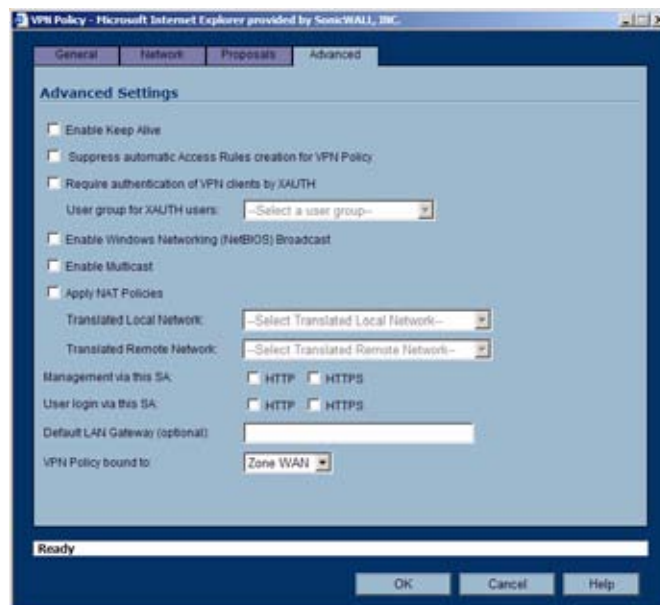


**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

**Step 13** Under **IPsec (Phase 2) Proposal**, the default values for **Protocol**, **Encryption**, **Authentication**, **Enable Perfect Forward Secrecy**, **DH Group**, and **Lifetime** are acceptable for most VPN SA configurations. Be sure the Phase 2 values on the opposite side of the tunnel are configured to match.

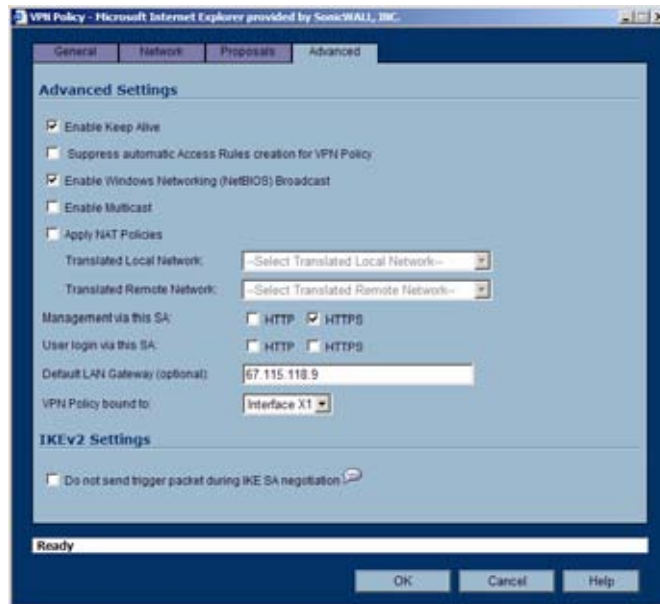
**Step 14** Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:

- If you selected **Main Mode** or **Aggressive Mode** in the **Proposals** tab:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or Zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

- If you selected **IKEv2** in the **Proposals** tab:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- Select **Suppress automatic Access Rules creation for VPN Policy** to turn off the automatic access rules created between the LAN and VPN zones for this VPN policy.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow IP multicasting traffic, such as streaming audio (including VoIP) and video applications, to pass through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.
- Enter the **Default LAN Gateway** if you have more than one gateway and you want this one always to be used first.
- Select an interface or Zone from the **VPN Policy bound to** menu. A **Zone WAN** is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.
- Under **IKEv2 Settings** (visible only if you selected **IKEv2** for **Exchange** on the **Proposals** tab), The **Do not send trigger packet during IKE SA negotiation** checkbox is cleared by default and should only be selected when required for interoperability.

The term *Trigger Packet* refers to the use of initial *Traffic Selector* payloads populated with the IP addresses from the packet that caused SA negotiation to begin. It is recommended practice to include *Trigger Packets* to assist the IKEv2 Responder in selecting the correct protected IP address ranges from its Security Policy Database. Not all implementations support this feature, so it may be appropriate to disable the inclusion of *Trigger Packets* to some IKE peers.

**Step 15** Click **OK**.

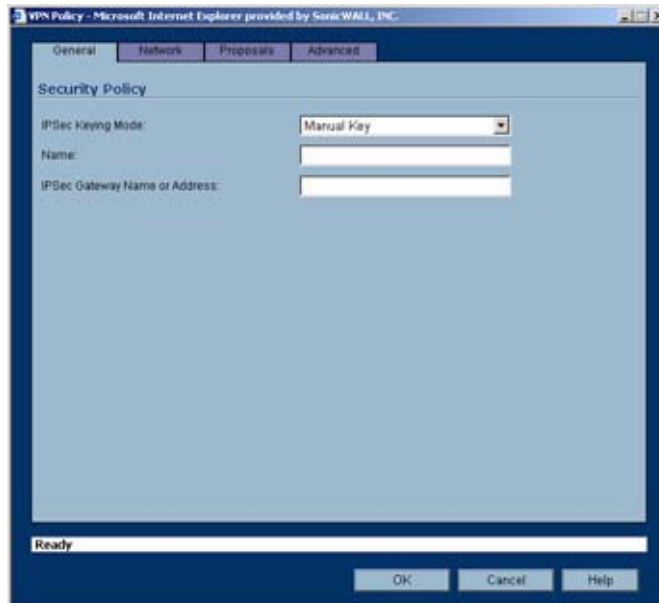
## **Configuring a VPN Policy using Manual Key**

To manually configure a VPN policy between two SonicWALL appliances using Manual Key, follow the steps below:

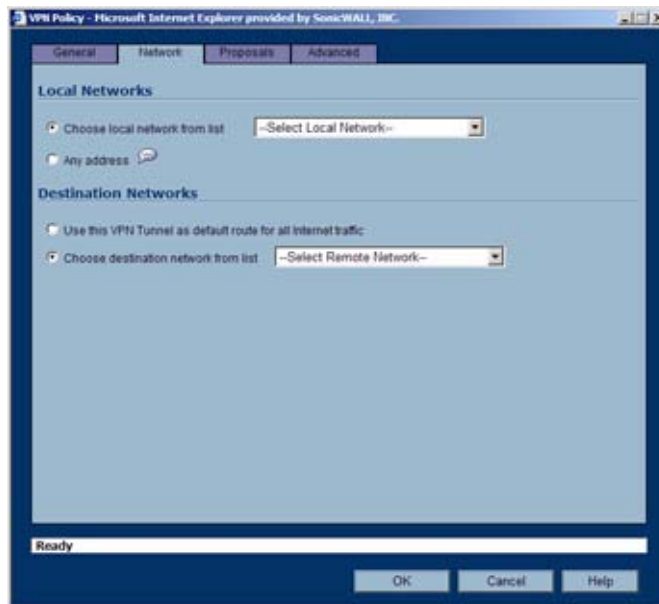


## Configuring the Local SonicWALL Security Appliance

- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- Step 2** In the **General** tab of the **VPN Policy** window, select **Manual Key** from the **IPsec Keying Mode** menu. The **VPN Policy** window displays the manual key options.



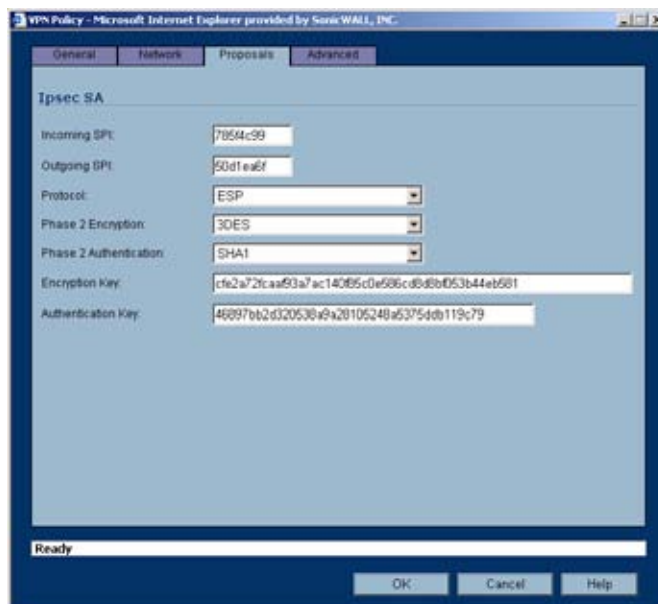
- Step 3** Enter a name for the policy in the **Name** field.
- Step 4** Enter the host name or IP address of the remote connection in the **IPsec Gateway Name or Address** field.
- Step 5** Click the **Network** tab.



- Step 6** Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Use this option if a peer has **Use this VPN Tunnel as default route for all Internet traffic** selected. You can only configure one SA to use this setting. Alternatively, select **Choose**

**Destination network from list**, and select the address object or group.

**Step 7** Click on the **Proposals** tab.



**Step 8** Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.

**Caution** Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.

**Step 9** The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.



**Note** The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.

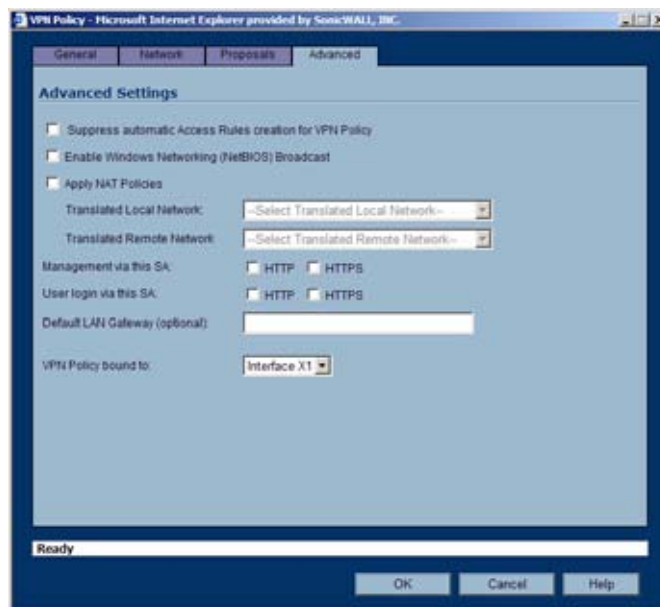
**Step 10** Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the SonicWALL.

**Step 11** Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the SonicWALL settings.

**Tip**

Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARC4 encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

**Step 12** Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy.



- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- To manage the local SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**.
- Select **HTTP**, **HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

**Step 13** Click **OK**.

**Step 14** Click **Apply** on the **VPN > Settings** page to update the VPN Policies.

## Configuring the Remote SonicWALL Security Appliance

- 
- Step 1** Click **Add** on the **VPN > Settings** page. The **VPN Policy** window is displayed.
- Step 2** In the **General** tab, select **Manual Key** from the **IPsec Keying Mode** menu.
- Step 3** Enter a name for the SA in the **Name** field.
- Step 4** Enter the host name or IP address of the local connection in the **IPsec Gateway Name or Address** field.
- Step 5** Click the **Network** tab.
- Step 6** Select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If traffic can originate from any local network, select **Any Address**. Select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. Alternatively, select **Choose Destination network from list**, and select the address object or group.
- Step 7** Click the **Proposals** tab.
- Step 8** Define an **Incoming SPI** and an **Outgoing SPI**. The SPIs are hexadecimal (0123456789abcdef) and can range from 3 to 8 characters in length.



### Warning

**Each Security Association must have unique SPIs; no two Security Associations can share the same SPIs. However, each Security Association Incoming SPI can be the same as the Outgoing SPI.**

- Step 9** The default values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** are acceptable for most VPN SA configurations.



### Note

The values for **Protocol**, **Phase 2 Encryption**, and **Phase 2 Authentication** must match the values on the remote SonicWALL.

- Step 10** Enter a 16 character hexadecimal encryption key in the **Encryption Key** field or use the default value. This encryption key is used to configure the remote SonicWALL encryption key, therefore, write it down to use when configuring the remote SonicWALL.
- Step 11** Enter a 32 character hexadecimal authentication key in the **Authentication Key** field or use the default value. Write down the key to use while configuring the remote SonicWALL settings.



### Tip

Valid hexadecimal characters include 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, and f. 1234567890abcdef is an example of a valid DES or ARCFour encryption key. If you enter an incorrect encryption key, an error message is displayed at the bottom of the browser window.

- Step 12** Click the **Advanced** tab and select any of the following optional settings you want to apply to your VPN policy:
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
  - Select **Enable Windows Networking (NetBIOS) broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.

- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** drop-down box. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** drop-down box. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.



Warning

---

**You cannot use this feature if you have selected Use this VPN Tunnel as the default route for all Internet traffic on the Network tab.**

---

- To manage the remote SonicWALL through the VPN tunnel, select **HTTP, HTTPS**, or both from **Management via this SA**.
- Select **HTTP, HTTPS**, or both in the **User login via this SA** to allow users to login using the SA.
- If you have an IP address for a gateway, enter it into the **Default LAN Gateway (optional)** field.
- Select an interface from the **VPN Policy bound to** menu.

**Step 13** Click **OK**.

**Step 14** Click **Apply** on the **VPN > Settings** page to update the VPN Policies.



Tip

---

Since Window Networking (NetBIOS) has been enabled, users can view remote computers in their Windows Network Neighborhood. Users can also access resources on the remote LAN by entering servers' or workstations' remote IP addresses.

---

## Configuring a VPN Policy with IKE using a Third Party Certificate



Warning

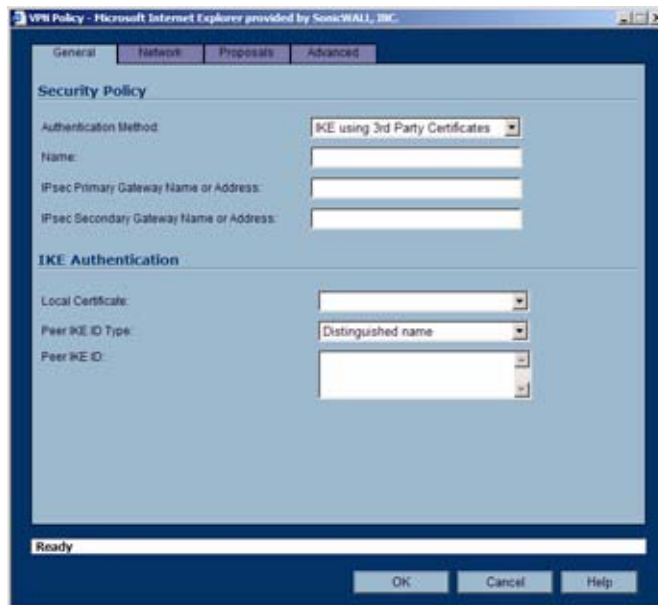
---

**You must have a valid certificate from a third party Certificate Authority installed on your SonicWALL before you can configure your VPN policy with IKE using a third party certificate.**

---

To create a VPN SA using IKE and third party certificates, follow these steps:

- Step 1** In the **VPN > Settings** page, click **Add**. The **VPN Policy** window is displayed.
- Step 2** In the **Authentication Method** list in the **General** tab, select **IKE using 3rd Party Certificates**. The **VPN Policy** window displays the 3rd party certificate options.

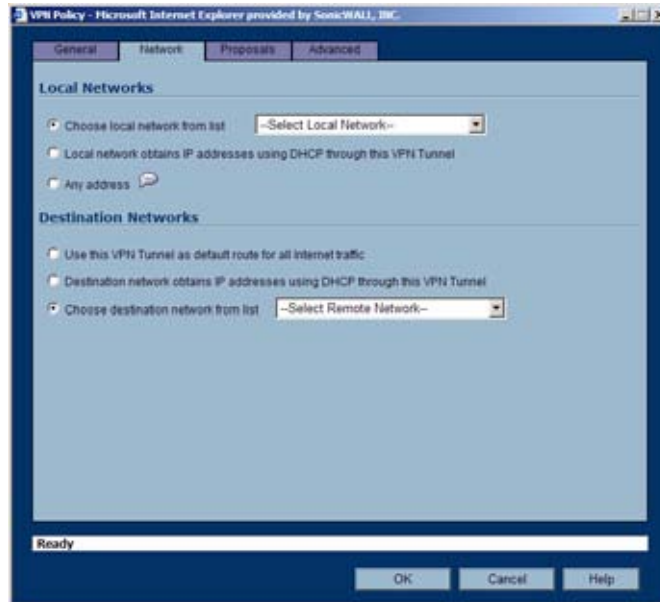


- Step 3** Type a Name for the Security Association in the **Name** field.
- Step 4** Type the IP address or Fully Qualified Domain Name (FQDN) of the primary remote SonicWALL in the **IPsec Primary Gateway Name or Address** field. If you have a secondary remote SonicWALL, enter the IP address or Fully Qualified Domain Name (FQDN) in the **IPsec Secondary Gateway Name or Address** field.
- Step 5** Under **IKE Authentication**, select a third party certificate from the **Local Certificate** list. You must have imported local certificates before selecting this option.
- Step 6** Select one of the following Peer ID types from the **Peer IKE ID Type** menu:
- **E-Mail ID and Domain Name** - The **Email ID** and **Domain Name** types are based on the certificate's Subject Alternative Name field, which is not contained in all certificates by default. If the certificate does not contain a Subject Alternative Name field, this filter will not work. The **E-Mail ID** and **Domain Name** filters can contain a string or partial string identifying the acceptable range required. The strings entered are not case sensitive and can contain the wild card characters \* (for more than 1 character) and ? (for a single character). For example, the string \*@sonicwall.com when **E-Mail ID** is selected, would allow anyone with an email address that ended in sonicwall.com to have access; the string \*sv.us.sonicwall.com when Domain Name is selected, would allow anyone with a domain name that ended in sv.us.sonicwall.com to have access.
  - **Distinguished Name** - Based on the certificates Subject Distinguished Name field, which is contained in all certificates by default. Valid entries for this field are based on country (c=), organization (o=), organization unit (ou=), and /or commonName (cn=).

Up to three organizational units can be specified. The usage is `c=*;o=*;ou=*;ou=*;ou=*;cn=*`. The final entry does not need to contain a semi-colon. You must enter at least one entry, i.e. `c=us`.

**Step 7** Type an ID string in the **Peer IKE ID** field.

**Step 8** Click on the **Network** tab.



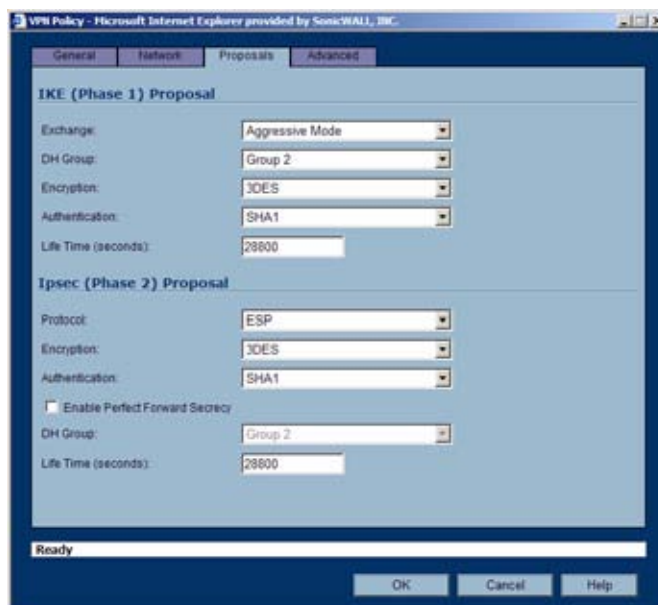
**Step 9** Under **Local Networks**, select a local network from **Choose local network from list** if a specific local network can access the VPN tunnel. If hosts on this side of the VPN connection will be obtaining their addressing from a DHCP server on the remote side of the tunnel, select **Local network obtains IP addresses using DHCP through this VPN tunnel**. If traffic can originate from any local network, select **Any Address**.

**Step 10** Under **Destination Networks**, select **Use this VPN Tunnel as default route for all Internet traffic** if traffic from any local user cannot leave the SonicWALL security appliance unless it is encrypted. You can only configure one SA to use this setting. If the remote side of this VPN connection is be obtaining its addressing from a DHCP server on this side of the tunnel, select

**Destination network obtains IP addresses using DHCP server through this tunnel.**

Alternatively, select **Choose Destination network from list**, and select the address object or group.

**Step 11** Click the **Proposals** tab.



**Step 12** In the **IKE (Phase 1) Proposal** section, select the following settings:

- Select **Main Mode** or **Aggressive Mode** from the **Exchange** menu.
- Select the desired DH Group from the **DH Group** menu.



**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.

- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

**Step 13** In the **IPsec (Phase 2) Proposal** section, select the following settings:

- Select the desired protocol from the **Protocol** menu.
- Select **3DES**, **AES-128**, **AES-192**, or **AES-256** from the **Encryption** menu.
- Select the desired authentication method from the **Authentication** menu.
- Select **Enable Perfect Forward Secrecy** if you want an additional Diffie-Hellman key exchange as an added layer of security. Select **Group 2** from the **DH Group** menu.

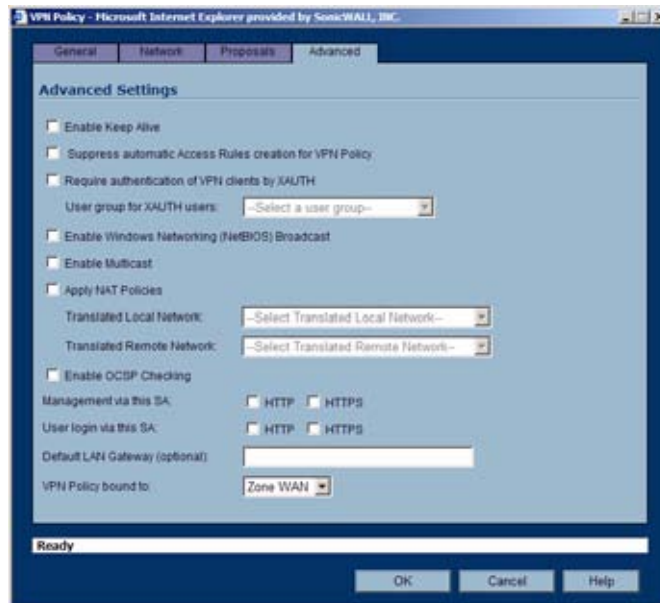


**Note** The Windows 2000 L2TP client and Windows XP L2TP client can only work with DH Group 2. They are incompatible with DH Groups 1 and 5.



- Enter a value in the **Life Time (seconds)** field. The default setting of **28800** forces the tunnel to renegotiate and exchange keys every 8 hours.

**Step 14** Click the **Advanced** tab. Select any optional configuration options you want to apply to your VPN policy:



- Select **Enable Keep Alive** to use heartbeat messages between peers on this VPN tunnel. If one end of the tunnel fails, using Keepalives will allow for the automatic renegotiation of the tunnel once both sides become available again without having to wait for the proposed Life Time to expire.
- The **Suppress automatic Access Rules creation for VPN Policy** setting is not enabled by default to allow the VPN traffic to traverse the appropriate zones.
- To require XAUTH authentication by users prior to allowing traffic to traverse this tunnel, select **Require authentication of VPN client by XAUTH**, and select a User group to specify allowed users from the **User group for XAUTH**.
- Select **Enable Windows Networking (NetBIOS) Broadcast** to allow access to remote network resources by browsing the Windows® Network Neighborhood.
- Select **Enable Multicast** to allow multicast traffic through the VPN tunnel.
- Select **Apply NAT Policies** if you want the SonicWALL to translate the Local, Remote or both networks communicating via this VPN tunnel. To perform Network Address Translation on the Local Network, select or create an Address Object in the **Translated Local Network** menu. To translate the Remote Network, select or create an Address Object in the **Translated Remote Network** menu. Generally, if NAT is required on a tunnel, either Local or Remote should be translated, but not both. **Apply NAT Policies** is particularly useful in cases where both sides of a tunnel use either the same or overlapping subnets.
- Select **Enable OCSP Checking** to check VPN certificate status and specify the URL where to check certificate status. See the [“Using OCSP with SonicWALL Security Appliances”](#) section in the [“VPN > Settings”](#) section on page 537.
- To manage the remote SonicWALL through the VPN tunnel, select **HTTP**, **HTTPS**, or both from **Management via this SA**. Select **HTTP**, **HTTPS**, or both in the User login via this SA to allow users to login using the SA.

- If you wish to use a router on the LAN for traffic entering this tunnel destined for an unknown subnet, for example, if you configured the other side to **Use this VPN Tunnel as default route for all Internet traffic**, you should enter the IP address of your router into the **Default LAN Gateway (optional)** field.
- Select an interface or Zone from the **VPN Policy bound to** menu. A Zone is the preferred selection if you are using WAN Load Balancing and you wish to allow the VPN to use either WAN interface.

Step 15 Click **OK**.

## VPN Auto-Added Access Rule Control

When adding VPN Policies, SonicOS Enhanced auto-creates non-editable Access Rules to allow the traffic to traverse the appropriate Zones. Consider the following VPN Policy, where the Local Network is set to Firewalled Subnets (in this case comprising the LAN and DMZ) and the Destination Network is set to Subnet 192.168.169.0. The VPN Policy appears as follows:

Name	Gateway	Destinations	Crypto Suite	Enable	Configure
Remote Site 1	87.115.118.80	192.168.169.1 - 192.168.169.255	ESP 3DES+HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

And the following Access Rules are added for inbound and outbound traffic:

Zone	Zone	Priority	Source	Destination	Service	Action	Users	Comment	Enable	Configure
DMZ	DMZ	1	Firewalled Subnets	Subnet 192.168.169.0	Any	allow	all		<input checked="" type="checkbox"/>	
LAN	LAN	1	Firewalled Subnets	Subnet 192.168.169.0	Any	allow	all		<input checked="" type="checkbox"/>	
VPN	LAN	3	Subnet 192.168.169.0	Firewalled Subnets	Any	allow	all		<input checked="" type="checkbox"/>	
VPN	DMZ	3	Subnet 192.168.169.0	Firewalled Subnets	Any	allow	all		<input checked="" type="checkbox"/>	

While this is generally a tremendous convenience, there are some instances where it might be preferable to suppress the auto-creation of Access Rules in support of a VPN Policy. One such instance would be the case of a large hub-and-spoke VPN deployment where all the spoke sites are addresses using address spaces that can easily be supernetted. For example, assume we wanted to provide access to/from the LAN and DMZ at the hub site to one subnet at each of 2,000 remote sites, addressed as follows:

```
remoteSubnet0=Network 10.0.0.0/24 (mask 255.255.255.0, range 10.0.0.0-10.0.0.255)
remoteSubnet1=Network 10.0.1.0/24 (mask 255.255.255.0, range 10.0.1.0-10.0.1.255)
remoteSubnet2=Network 10.0.2.0/24 (mask 255.255.255.0, range 10.0.2.0-10.0.2.255)
remoteSubnet2000=10.7.207.0/24 (mask 255.255.255.0, range 10.7.207.0-10.7.207.255)
```

Creating VPN Policies for each of these remote sites would result in the requisite 2,000 VPN Policies, but would also create 8,000 Access Rules (LAN -> VPN, DMZ -> VPN, VPN -> LAN, and VPN -> DMZ for each site). However, all of these Access Rules could easily be handled with just 4 Access Rules to a supernetted or address range representation of the remote sites (More specific allow or deny Access Rules could be added as needed):

```
remoteSubnetAll=Network 10.0.0.0/13 (mask 255.248.0.0, range 10.0.0.0-10.7.255.255)
or
remoteRangeAll=Range 10.0.0.0-10.7.207.255
```

To enable this level of aggregation, the **Advanced** tab of the **VPN Policy** window page offers the option to **Auto-Add Access Rules for VPN Policy** setting. By default, the checkbox is selected, meaning the accompanying Access Rules will be automatically created, as they've always been. By deselecting the checkbox upon creating the VPN Policy, the administrator will have the ability and need to create custom Access Rules for VPN traffic.





# CHAPTER 49

## Configuring Advanced VPN Settings

### VPN > Advanced

The **VPN > Advanced** page includes optional settings that affect all VPN policies.

The screenshot shows the 'VPN > Advanced VPN Settings' configuration page. At the top right, there are 'Apply', 'Cancel', and '?' buttons. The page is divided into two main sections: 'Advanced VPN Settings' and 'IKEv2 Settings'. Under 'Advanced VPN Settings', there are several checkboxes and input fields: 'Enable IKE Dead Peer Detection' (checked), 'Dead Peer Detection Interval (seconds)' (60), 'Failure Trigger Level (missed heartbeats)' (3), 'Enable Dead Peer Detection for Idle VPN sessions' (unchecked), 'Dead Peer Detection Interval for Idle VPN sessions (seconds)' (600), 'Enable Fragmented Packet Handling' (checked), 'Ignore DF (Don't Fragment) Bit' (checked), 'Enable NAT Traversal' (checked), 'Clean up Active tunnels when Peer Gateway DNS name resolves to a different IP Address' (checked), 'Preserve IKE Port for Pass Through Connections' (unchecked), 'Enable OCSP Checking' (unchecked), 'Send VPN Tunnel Traps only when tunnel status changes' (unchecked), and 'Use RADIUS in MSCHAP mode for XAUTH (allows users to change expired passwords)' (unchecked). Under 'IKEv2 Settings', there is a checkbox for 'Send IKEv2 Cookie Notify' (unchecked) and a 'Configure...' button for 'IKEv2 Dynamic Client Proposal'.

### Advanced VPN Settings

- **Enable IKE Dead Peer Detection** - Select if you want inactive VPN tunnels to be dropped by the SonicWALL.

- **Dead Peer Detection Interval** - Enter the number of seconds between “heartbeats.” The default value is 60 seconds.
- **Failure Trigger Level (missed heartbeats)** - Enter the number of missed heartbeats. The default value is 3. If the trigger level is reached, the VPN connection is dropped by the SonicWALL security appliance. The SonicWALL security appliance uses a UDP packet protected by Phase 1 Encryption as the heartbeat.
- **Enable Dead Peer Detection for Idle VPN Sessions** - Select this setting if you want idle VPN connections to be dropped by the SonicWALL security appliance after the time value defined in the **Dead Peer Detection Interval for Idle VPN Sessions (seconds)** field. The default value is 600 seconds (10 minutes).
- **Enable Fragmented Packet Handling** - If the VPN log report shows the log message “Fragmented IPsec packet dropped”, select this feature. Do not select it until the VPN tunnel is established and in operation.

**Ignore DF (Don't Fragment) Bit** - When you select **Enable Fragmented Packet Handling**, the **Ignore DF (Don't Fragment) Bit** setting becomes active.

- **Enable NAT Traversal** - Select this setting is a NAT device is located between your VPN endpoints. IPsec VPNs protect traffic exchanged between authenticated endpoints, but authenticated endpoints cannot be dynamically re-mapped mid-session for NAT traversal to work. Therefore, to preserve a dynamic NAT binding for the life of an IPsec session, a 1-byte UDP is designated as a “NAT Traversal keepalive” and acts as a “heartbeat” sent by the VPN device behind the NAT or NAPT device. The “keepalive” is silently discarded by the IPsec peer.
- **Clean up Active Tunnels when Peer Gateway DNS names resolves to a different IP address** - Breaks down SAs associated with old IP addresses and reconnects to the peer gateway.
- **Preserve IKE Port for Pass-Through Connections** - Preserves UDP 500/4500 source port and IP address information for pass-through VPN connections.
- **Enable OCSP Checking and OCSP Responder URL** - Enables use of Online Certificate Status Protocol (OCSP) to check VPN certificate status and specifies the URL where to check certificate status. See [Using OCSP with SonicWALL Security Appliances](#).
- **Send IKEv2 Cookie Notify** - Sends cookies to IKEv2 peers as an authentication tool.
- **Use RADIUS in** - When using RADIUS to authenticate VPN client users, RADIUS will be used in its MSCHAP (or MSCHAPv2) mode. The primary reason for choosing to do this would be so that VPN client users can make use of the MSCHAP feature to allow them to change expired passwords at login time.

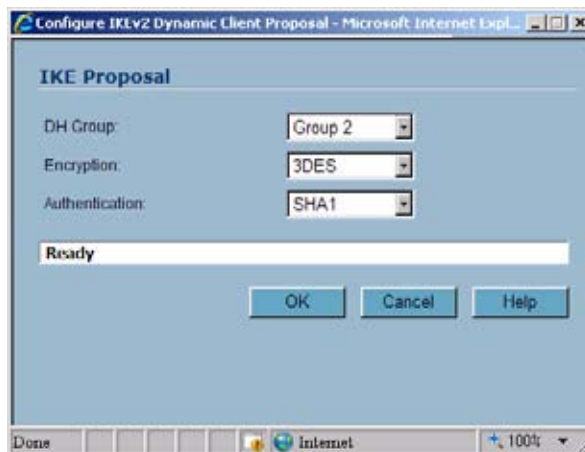
Also if this is set and LDAP is selected as the **Authentication method for login** on the **Users > Settings** page, but LDAP is not configured in a way that will allow password updates, then password updates for VPN client users will be done using MSCHAP-mode RADIUS after using LDAP to authenticate the user.



**Note**

Password updates can only be done by LDAP when using Active Directory with TLS and binding to it using an administrative account, or when using Novell eDirectory.

- **IKEv2 Dynamic Client Proposal** - SonicOS Enhanced 4.0 introduces IKEv2 Dynamic Client Support, which provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Clicking the **Configure** button launches the **Configure IKEv2 Dynamic Client Proposal** window.



Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:

- **DH Group:** 1, 2, or 5
- **Encryption:** DES, 3DES, AES-128, AES-192, AES-256
- **Authentication:** MD5, SHA1

However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.



**Note** The VPN policy on the remote gateway must also be configured with the same settings.

## Using OCSP with SonicWALL Security Appliances

Online Certificate Status Protocol (OCSP) allows you to check VPN certificate status without CRLs. This allows timely updates regarding the status of the certificates used on your SonicWALL.

### About OCSP

OCSP is designed to augment or replace Certificate Revocation Lists (CRL) in your Public Key Infrastructure (PKI) or digital certificate system. The CRL is used to validate the digital certificates comprised by the PKI. This allows the Certificate Authority (CA) to revoke certificates before their scheduled expiration date and is useful in protecting the PKI system against stolen or invalid certificates.

Certificate Revocation Lists main disadvantage is the need for frequent updates to keep the CRL of every client current. These frequent updates greatly increase network traffic when the complete CRL is downloaded by every client. Depending on the frequency of the CRL updates, a period of time can exist when a certificate is revoked by the CRL but the client has not received the CRL update and permits the certificate to be used.

Online Certificate Status Protocol determines the current status of a digital certificate without using a CRL. OCSP enables the client or application to directly determine the status of an identified digital certificate. This provides more timely information about the certificate than is possible with CRLs. In addition, each client typically only checks a few certificates and does not incur the overhead of downloading an entire CRL for only a few entries. This greatly reduces the network traffic associated with certificate validation.

OCSP transports messages over HTTP for maximum compatibility with existing networks. This requires careful configuration of any caching servers in the network to avoid receiving a cached copy of an OCSP response that might be out of date.

The OCSP client communicates with an OCSP responder. The OCSP responder can be a CA server or another server that communicates with the CA server to determine the certificate status. The OCSP client issues a status request to an OCSP responder and suspends the acceptance of the certificate until the responder provides a response. The client request includes data such as protocol version, service request, target certificate identification and optional extensions. These optional extensions may or may not be acknowledged by the OCSP responder.

The OCSP responder receives the request from the client and checks that the message is properly formed and if the responder is able to respond to the service request. Then it checks if the request contains the correct information needed for the service desired. If all conditions are satisfied, the responder returns a definitive response to the OCSP client. The OCSP responder is required to provide a basic response of GOOD, REVOKED, or UNKNOWN. If both the OCSP client and responder support the optional extensions, other responses are possible. The GOOD state is the desired response as it indicates the certificate has not been revoked. The REVOKED state indicates that the certificate has been revoked. The UNKNOWN state indicates the responder does not have information about the certificate in question.

OCSP servers typically work with a CA server in push or pull setup. The CA server can be configured to push a CRL list (revocation list) to the OCSP server. Additionally the OCSP server can be configured to periodically download (pull) the CRL from the CA server. The OCSP server must also be configured with an OCSP response signing certificate issued by the CA server. The signing certificate must be properly formatted or the OCSP client will not accept the response from the OSCP server.

## OpenCA OCSP Responder

Using OCSP requires the OpenCA (OpenSource Certificate Authority) OpenCA OCSP Responder as it is the only supported OCSP responder. OpenCA OCSP Responder is available at <http://www.openca.org/ocspd/>. The OpenCA OCSP Responder is an rfc2560 compliant OCSP responder that runs on a default port of 2560 in homage to being based on rfc2560.

## Loading Certificates to use with OCSP

For SonicOS to act as an OCSP client to a responder, the CA certificate must be loaded onto the SonicWALL.

- 
- Step 1** On the **System** -> **Certificates** page, click on the Import button. This will bring up the Import Certificate page.
  - Step 2** Select the **Import a CA certificate from a PKCS#7 (.p7b), PEM (.pem) or DER (.der or .cer) encoded file** option and specify the location of the certificate.



## Using OCSP with VPN Policies

The SonicWALL OCSP settings can be configured on a policy level or globally. To configure OCSP checking for individual VPN policies, use the **Advanced** tab of the **VPN Policy** configuration page.

- 
- Step 1** Select the radio button next to **Enable OCSP Checking**.
  - Step 2** Specify the **OCSP Responder URL** of the OCSP server, for example <http://192.168.168.220:2560> where 192.168.168.220 is the IP address of your OCSP server and 2560 is the default port of operation for the OpenCA OCSP responder service.



# CHAPTER 50

## Configuring DHCP Over VPN

### VPN > DHCP over VPN

The **VPN > DHCP over VPN** page allows you to configure a SonicWALL security appliance to obtain an IP address lease from a DHCP server at the other end of a VPN tunnel. In some network deployments, it is desirable to have all VPN networks on one logical IP subnet, and create the appearance of all VPN networks residing in one IP subnet address space. This facilitates IP address administration for the networks using VPN tunnels.



### DHCP Relay Mode

The SonicWALL security appliance at the remote and central site are configured for VPN tunnels for initial DHCP traffic as well as subsequent IP traffic between the sites. The SonicWALL security appliance at the remote site (**Remote Gateway**) passes DHCP broadcast packets through its VPN tunnel. The SonicWALL security appliance at the central site (**Central Gateway**) relays DHCP packets from the client on the remote network to the DHCP server on the central site.

## Configuring the Central Gateway for DHCP Over VPN

To configure **DHCP over VPN** for the **Central Gateway**, use the following steps:

1. Select **VPN > DHCP over VPN**.
2. Select **Central Gateway** from the **DHCP Relay Mode** menu.
3. Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



4. Select **Use Internal DHCP Server** to enable the SonicWALL Global VPN Client or a remote firewall or both to use an internal DHCP server to obtain IP addressing information. Check the **For Global VPN Client** checkbox to use the DHCP Server for Global VPN Clients and check the **For Remote Firewall** checkbox for the SonicWALL Global Security Client's firewall.
5. If you want to send DHCP requests to specific servers, select **Send DHCP requests to the server addresses listed below**.
6. Click **Add**. The **Add DHCP Server** window is displayed.



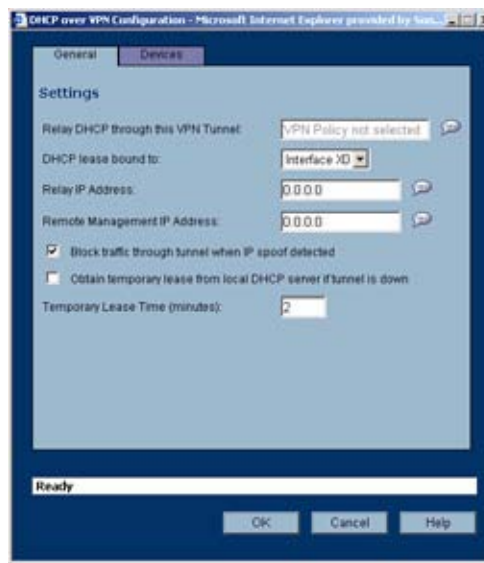
7. Type the IP addresses of DHCP servers in the **IP Address** field, and click **OK**. The SonicWALL security appliance now directs DHCP requests to the specified servers.
8. Type the IP address of a relay server in the **Relay IP Address (Optional)** field.

To edit an entry in the **IP Address** table, click **Edit**. To delete a DHCP Server, highlight the entry in the **IP Address** table, and click **Delete**. Click **Delete All** to delete all entries.

## Configuring DHCP over VPN Remote Gateway

1. Select **Remote Gateway** from the **DHCP Relay Mode** menu.

- Click **Configure**. The **DHCP over VPN Configuration** window is displayed.



- In the **General** tab, the VPN policy name is automatically displayed in the Relay DHCP through this VPN Tunnel field if the VPN policy has the setting **Local network obtains IP addresses using DHCP through this VPN Tunnel** enabled.



**Note**

Only VPN policies using IKE can be used as VPN tunnels for DHCP.

- Select the interface the DHCP lease is bound from the **DHCP lease bound to** menu.
- If you enter an IP address in the **Relay IP address** field, this IP address is used as the DHCP Relay Agent IP address in place of the Central Gateway's address, and must be reserved in the DHCP scope on the DHCP server. This address can also be used to manage this SonicWALL security appliance remotely through the VPN tunnel from behind the Central Gateway.
- If you enter an IP address in the **Remote Management IP Address** field, this IP address is used to manage the SonicWALL security appliance from behind the Central Gateway, and must be reserved in the DHCP scope on the DHCP server.
- If you enable **Block traffic through tunnel when IP spoof detected**, the SonicWALL security appliance blocks any traffic across the VPN tunnel that is spoofing an authenticated user's IP address. If you have any static devices, however, you must ensure that the correct Ethernet address is typed for the device. The Ethernet address is used as part of the identification process, and an incorrect Ethernet address can cause the SonicWALL security appliance to respond to IP spoofs.
- If the VPN tunnel is disrupted, temporary DHCP leases can be obtained from the local DHCP server. Once the tunnel is again active, the local DHCP server stops issuing leases. Enable the **Obtain temporary lease from local DHCP server if tunnel is down** check box. By enabling this check box, you have a failover option in case the tunnel ceases to function. If you want to allow temporary leases for a certain time period, type the number of minutes for the temporary lease in the **Temporary Lease Time** box. The default value is 2 minutes.

## Devices

- To configure devices on your LAN, click the **Devices** tab.



- To configure **Static Devices on the LAN**, click **Add** to display the **Add LAN Device Entry** window, and type the IP address of the device in the **IP Address** field and then type the Ethernet address of the device in the **Ethernet Address** field.



An example of a static device is a printer as it cannot obtain an IP lease dynamically. If you do not have **Block traffic through tunnel when IP spoof detected** enabled, it is not necessary to type the Ethernet address of a device. You must exclude the Static IP addresses from the pool of available IP addresses on the DHCP server so that the DHCP server does not assign these addresses to DHCP clients. You should also exclude the IP address used as the **Relay IP Address**. It is recommended to reserve a block of IP address to use as Relay IP addresses. Click **OK**.

- To exclude devices on your LAN, click **Add** to display the **Add Excluded LAN Entry** window. Enter the MAC address of the device in the **Ethernet Address** field. Click **OK**.



- Click **OK** to exit the **DHCP over VPN Configuration** window.

**Note**

You must configure the local DHCP server on the remote SonicWALL security appliance to assign IP leases to these computers.

**Note**

If a remote site has trouble connecting to a central gateway and obtaining a lease, verify that Deterministic Network Enhancer (DNE) is not enabled on the remote computer.

**Tip**

If a static LAN IP address is outside of the DHCP scope, routing is possible to this IP, i.e. two LANs.

## Current DHCP over VPN Leases

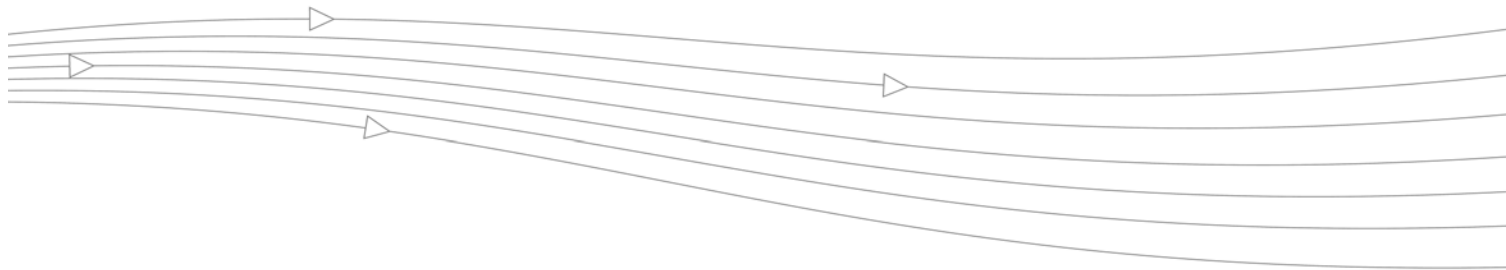
The scrolling window shows the details on the current bindings: IP and Ethernet address of the bindings, along with the Lease Time, and Tunnel Name.

To delete a binding, which frees the IP address in the DHCP server, select the binding from the list, and then click the **Trash** icon. The operation takes a few seconds to complete. Once completed, a message confirming the update is displayed at the bottom of the Web browser window.

Click **Delete All** to delete all VPN leases.







# CHAPTER 51

## Configuring L2TP Server

---

### VPN > L2TP Server

The SonicWALL security appliance can terminate L2TP-over-IPsec connections from incoming Microsoft Windows 2000 and Windows XP clients. In situations where running the SonicWALL Global VPN Client is not possible, you can use the SonicWALL L2TP Server to provide secure access to resources behind the SonicWALL security appliances.

You can use Layer 2 Tunneling Protocol (L2TP) to create VPN over public networks such as the Internet. L2TP provides interoperability between different VPN vendors that protocols such as PPTP and L2F do not, although L2TP combines the best of both protocols and is an extension of them. L2TP is supported on Microsoft Windows 2000 Operating System.

L2TP supports several of the authentication options supported by PPP, including Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), and Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). You can use L2TP to authenticate the endpoints of a VPN tunnel to provide additional security, and you can implement it with IPsec to provide a secure, encrypted VPN solution.



**Note**

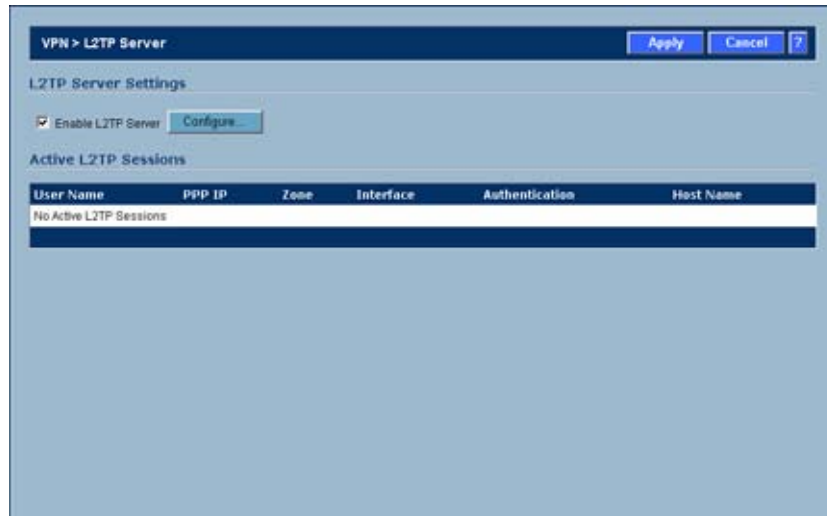
---

For more complete information on configuring the L2TP Server, see the technote **Configuring the L2TP Server in SonicOS** located on the SonicWALL documentation site: <http://www.sonicwall.com/us/Support.html>.

---

## Configuring the L2TP Server

The **VPN > L2TP Server** page provides the settings for configuring the SonicWALL security appliance as a L2TP Server.



To configure the L2TP Server, follow these steps:

1. To enable L2TP Server functionality on the SonicWALL security appliance, select **Enable L2TP Server**. Then click **Configure** to display the **L2TP Server Configuration** window.



2. Enter the number of seconds in the **Keep alive time (secs)** field to send special packets to keep the connection open. The default is **60** seconds.
3. Enter the IP address of your first DNS server in the **DNS Server 1** field. If you have a second DNS server, type the IP address in the **DNS Server 2** field.
4. Enter the IP address of your first WINS server in the **WINS Server 1** field. If you have a second WINS server, type the IP address in the **WINS Server 2** field.
5. Select **IP address provided by RADIUS Server** if a RADIUS Server provides IP addressing information to the L2TP clients.

6. If the L2TP Server provides IP addresses, select **Use the Local L2TP IP** pool. Enter the range of private IP addresses in the **Start IP** and **End IP** fields. The private IP addresses should be a range of IP addresses on the LAN.
7. If you have configured a specific user group defined for using L2TP, select it from the **User Group for L2TP users** menu or use **Everyone**.
8. Click **OK**.

## Currently Active L2TP Sessions

- **User Name** - The user name assigned in the local user database or the RADIUS user database.
- **PPP IP** - The source IP address of the connection.
- **Zone** - The zone used by the L2TP client.
- **Interface** - The type of interface used to access the L2TP Server, whether it's a VPN client or another SonicWALL security appliance.
- **Authentication** - Type of authentication used by the L2TP client.
- **Host Name** - The name of the network connecting to the L2TP Server.



# **PART 10**

# **User Management**





## CHAPTER 52

# Managing Users and Authentication Settings

---

## User Management

This chapter describes the user management capabilities of your SonicWALL security appliance for locally and remotely authenticated users. This chapter contains the following sections:

- [“Introduction to User Management” on page 599](#)
- [“Viewing Status on Users > Status” on page 613](#)
- [“Configuring Settings on Users > Settings” on page 614](#)
- [“Configuring Local Users” on page 618](#)
- [“Configuring Local Groups” on page 621](#)
- [“Configuring RADIUS Authentication” on page 625](#)
- [“Configuring LDAP Integration in SonicOS Enhanced” on page 631](#)
- [“Configuring Single Sign-On” on page 641](#)
- [“Configuring Multiple Administrator Support” on page 670](#)

## Introduction to User Management

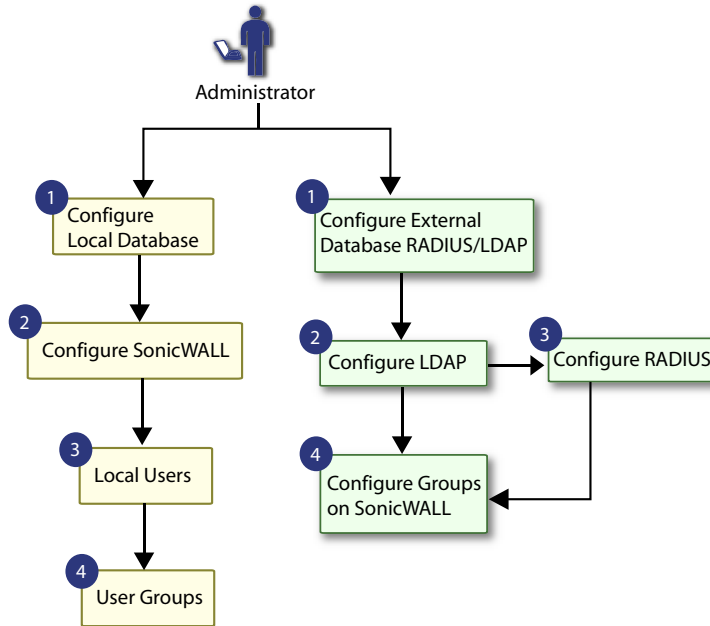
See the following sections for more information:

- [“Using Local Users and Groups for Authentication” on page 600](#)
- [“Using RADIUS for Authentication” on page 602](#)
- [“Using LDAP / Active Directory / eDirectory Authentication” on page 602](#)
- [“Single Sign-On Overview” on page 605](#)
- [“Multiple Administrator Support Overview” on page 610](#)

SonicWALL security appliances provide a mechanism for user level authentication that gives users access to the LAN from remote locations on the Internet as well as a means to enforce or bypass content filtering policies for LAN users attempting to access the Internet. You can also permit only authenticated users to access VPN tunnels and send data across the

encrypted connection. The SonicWALL authenticates all users as soon as they attempt to access network resources in a different zone (such as WAN, VPN, WLAN, etc), which causes the network traffic to pass through the SonicWALL. Users who log into a computer on the LAN, but perform only local tasks are not authenticated by the SonicWALL. User level authentication can be performed using a local user database, LDAP, RADIUS, or a combination of a local database with either LDAP or RADIUS. SonicOS also provides Single Sign-On (SSO) capability. SSO can be used in conjunction with LDAP. The local database on the SonicWALL can support up to 1000 users. If you have more than 1000 users, you must use LDAP or RADIUS for authentication.

**Figure 52:1 User Management Flow Diagram**

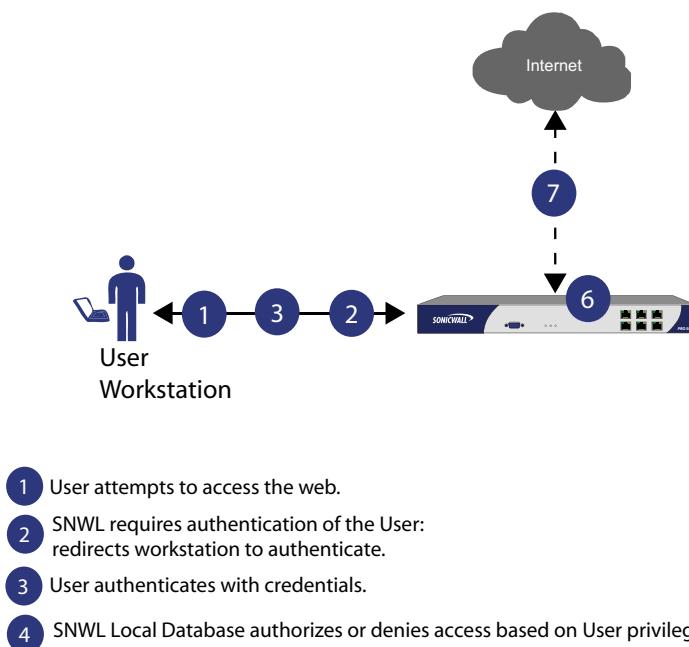


## Using Local Users and Groups for Authentication

The SonicWALL security appliance provides a local database for storing user and group information. You can configure the SonicWALL to use this local database to authenticate users and control their access to the network. The local database is a good choice over LDAP or RADIUS for this purpose when the number of users accessing the network is relatively small. Creating entries for dozens of users and groups takes time, although once the entries are in place they are not difficult to maintain. For networks with larger numbers of users, user authentication using LDAP or RADIUS servers can be more efficient.



**Figure 52:2 Local Groups Authentication Flow Diagram**



To apply Content Filtering Service (CFS) policies to users, the users must be members of local groups and the CFS policies are then applied to the groups. To use CFS, you cannot use LDAP or RADIUS without combining that method with local authentication. When using the combined authentication method in order to use CFS policies, the local group names must be an exact match with the LDAP or RADIUS group names. When using the **LDAP + Local Users** authentication method, you can import the groups from the LDAP server into the local database on the SonicWALL. This greatly simplifies the creation of matching groups, to which CFS policies can then be applied.

The SonicOS user interface provides a way to create local user and group accounts. You can add users and edit the configuration for any user, including settings for the following:

- Group membership - Users can belong to one or more local groups. By default, all users belong to the groups **Everyone** and **Trusted Users**. You can remove these group memberships for a user, and can add memberships in other groups.
- VPN access - You can configure the networks that are accessible to a VPN client started by this user. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their **Address Group** or **Address Object** names.

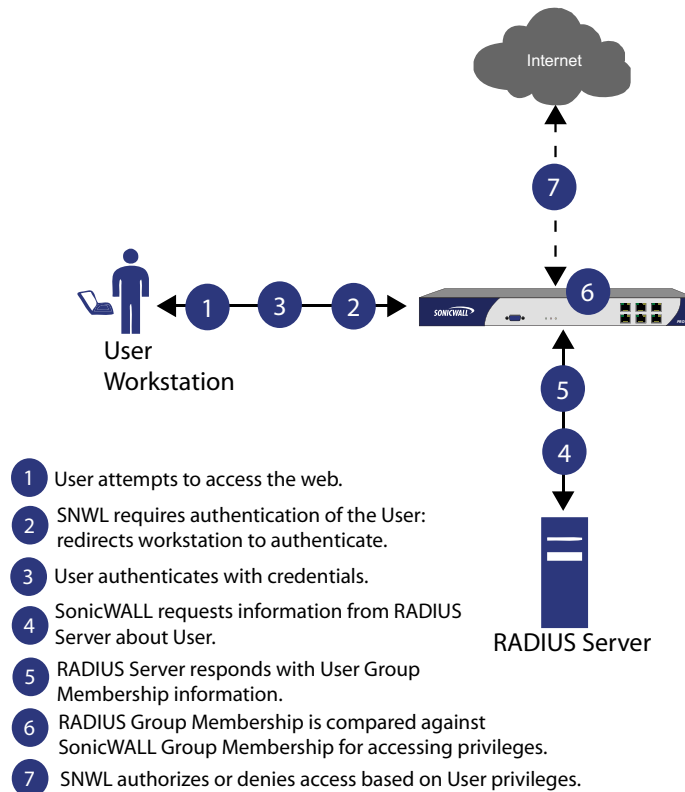
You can also add or edit local groups. The configurable settings for groups include the following:

- Group members - Groups have members that can be local users or other local groups.
- VPN access - VPN access for groups is configured in the same way as VPN access for users. You can configure the networks that are accessible to a VPN client started by a member of this group. When configuring VPN access settings, you can select from a list of networks. The networks are designated by their **Address Group** or **Address Object** names.
- CFS policy - You can apply a content filtering (CFS) policy to group members. The CFS policy setting is only available if the SonicWALL is currently licensed for Premium Content Filtering Service.

## Using RADIUS for Authentication

Remote Authentication Dial In User Service (RADIUS) is a protocol used by SonicWALL security appliances to authenticate users who are attempting to access the network. The RADIUS server contains a database with user information, and checks a user's credentials using authentication schemes such as Password Authentication Protocol (PAP), Challenge-handshake authentication protocol (CHAP), Microsoft CHAP (MSCHAP), or MSCHAPv2.

**Figure 52:3 RADIUS User Group Authentication Flow Diagram**

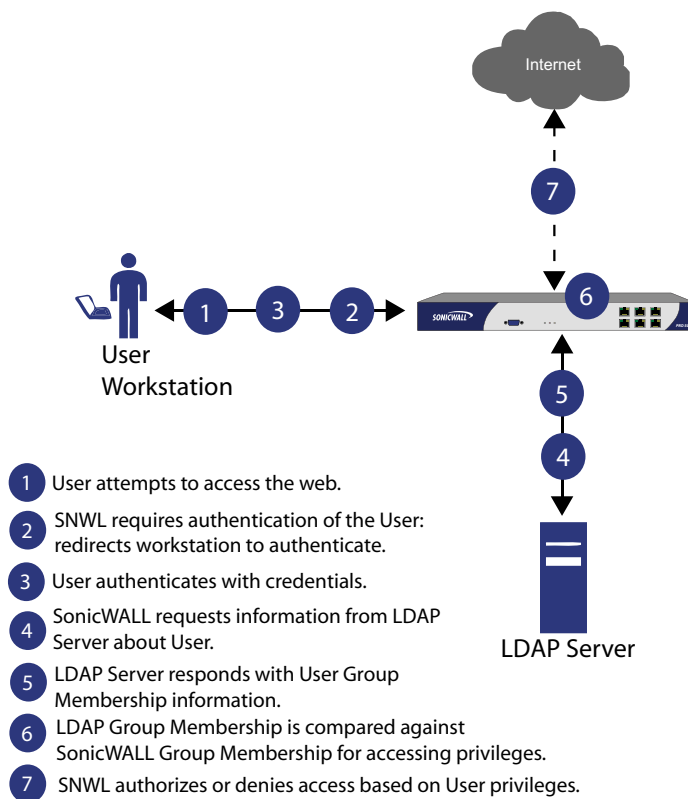


While RADIUS is very different from LDAP, it does provide a long list of attributes for each entry, including the user name, password, and domain. RADIUS can store information for thousands of users, and is a good choice for user authentication purposes when many users need access to the network.

## Using LDAP / Active Directory / eDirectory Authentication

Lightweight Directory Access Protocol (LDAP) defines a directory services structure for storing and managing information about elements in your network, such as user accounts, user groups, hosts, and servers. Several different standards exist that use LDAP to manage user account, group, and permissions. Some are proprietary systems like Microsoft Active Directory which you can manage using LDAP. Some are open standards SAMBA, which are implementations of the LDAP standards. Some are proprietary systems like Novell eDirectory which provide an LDAP API for managing the user repository information.

Figure 52:4 LDAP User Group Authentication Flow Diagram



In addition to RADIUS and the local user database, SonicOS Enhanced supports LDAP, Microsoft Active Directory (AD), and Novell eDirectory directory services for user authentication.

Microsoft Active Directory works with SonicWALL Single Sign-On and the SonicWALL SSO Agent. For more information, see [“Single Sign-On Overview”](#) on page 605.

### LDAP Directory Services Supported in SonicOS Enhanced

In order to integrate with the most common directory services used in company networks, SonicOS Enhanced supports integration with the following LDAP schemas:

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User-defined schemas

SonicOS Enhanced provides support for directory servers running the following protocols:

- LDAPv2 (RFC3494)
- LDAPv3 (RFC2251-2256, RFC3377)
- LDAPv3 over TLS (RFC2830)
- LDAPv3 with STARTTLS (RFC2830)
- LDAP Referrals (RFC2251)

## LDAP Terms

The following terms are useful when working with LDAP and its variants:

- *Schema* – The schema is the set of rules or the structure that defines the types of data that can be stored in a directory, and how that data can be stored. Data is stored in the form of ‘entries’.
- *Active Directory (AD)* – The Microsoft directory service, commonly used with Windows-based networking. Microsoft Active Directory is compatible with LDAP.
- *eDirectory* – The Novell directory service, used for Novell NetWare-based networking. Novell eDirectory has an LDAP gateway that can be used for management.
- *Entry* – The data that is stored in the LDAP directory. Entries are stored in ‘attribute’/value (or name/value) pairs, where the attributes are defined by ‘object classes’. A sample entry would be ‘cn=john’ where ‘cn’ (common name) is the attribute, and ‘john’ is the value.
- *Object class* – Object classes define the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be ‘user’ or ‘group’.

Microsoft Active Directory’s Classes can be browsed at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes\\_all.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/classes_all.asp)

- *Object* - In LDAP terminology, the entries in a directory are referred to as objects. For the purposes of the SonicOS implementation of the LDAP client, the critical objects are ‘User’ and ‘Group’ objects. Different implementations of LDAP can refer to these object classes in different fashions, for example, Active Directory refers to the user object as ‘user’ and the group object as ‘group’, while RFC2798 refers to the user object as ‘inetOrgPerson’ and the group object as ‘groupOfNames’.
- *Attribute* - A data item stored in an object in an LDAP directory. Object can have required attributes or allowed attributes. For example, the ‘dc’ attribute is a required attribute of the ‘dcObject’ (domain component) object.
- *dn* - A ‘distinguished name’, which is a globally unique name for a user or other object. It is made up of a number of components, usually starting with a common name (cn) component and ending with a domain specified as two or more domain components (dc). For example, ‘cn=john,cn=users,dc=domain,dc=com’
- *cn* – The ‘common name’ attribute is a required component of many object classes throughout LDAP.
- *ou* – The ‘organizational unit’ attribute is a required component of most LDAP schema implementations.
- *dc* – The ‘domain component’ attribute is commonly found at the root of a distinguished name, and is commonly a required attribute.
- *TLS* – Transport Layer Security is the IETF standardized version of SSL (Secure Sockets Layer). TLS 1.0 is the successor to SSL 3.0.

### Further Information on LDAP Schemas

- **Microsoft Active Directory:** Schema information is available at [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active\\_directory\\_schema.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/adschema/adschema/active_directory_schema.asp) and [http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap\\_reference.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/ldap/ldap/ldap_reference.asp)
- **RFC2798 InetOrgPerson:** Schema definition and development information is available at <http://rfc.net/rfc2798.html>
- **RFC2307 Network Information Service:** Schema definition and development information is available at <http://rfc.net/rfc2307.html>

- **Samba SMB:** Development information is available at <http://us5.samba.org/samba/>
- **Novell eDirectory:** LDAP integration information is available at <http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/h0000007.html>
- User-defined schemas: See the documentation for your LDAP installation. You can also see general information on LDAP at <http://rfc.net/rfc1777.html>

## Single Sign-On Overview

This section provides an introduction to the SonicWALL SonicOS Enhanced 4.0 Single Sign-On feature. This section contains the following subsections:

- “What Is Single Sign-On?” section on page 605
- “Benefits” section on page 606
- “How Does Single Sign-On Work?” section on page 607
- “Platforms” section on page 606

### What Is Single Sign-On?

Single Sign-On (SSO) is a transparent user authentication mechanism that provides privileged access to multiple network resources with a single workstation login. SonicWALL PRO and TZ series security appliances (SonicWALL security appliances) running SonicOS Enhanced 4.0 provide SSO functionality using the SonicWALL Single Sign-On Agent (SSO Agent) to identify user activity based on workstation IP address. SSO is configured in the **Users > Settings** page of the SonicOS management interface. SSO is separate from the **Authentication method for login** settings, which can be used at the same time for authentication of VPN/L2TP client users or administrative users.

SonicWALL SSO Agent identifies users by IP address using a SonicWALL ADConnector-compatible protocol and automatically determines when a user has logged out to prevent unauthorized access. Based on data from SonicWALL SSO Agent, the SonicWALL security appliance queries LDAP or the local database to determine group membership. Memberships are matched against policy, and based on user privileges, access is granted or denied. The configured inactivity and session limit timers apply with SSO, though users who are logged out are automatically and transparently logged back in when they send further traffic.

Users logged into a workstation directly but not logged into the domain will not be authenticated. For users that are not logged into the domain, the following screen will display, indicating that a manual login will be required for further authentication.



Users that are identified but lack the group memberships required by the configured policy rules are redirected to the Access Barred page.



## Benefits

SonicWALL SSO is a reliable and time-saving feature that utilizes a single login to provide access to multiple network resources based on administrator-configured group memberships and policy matching. SonicWALL SSO is transparent to end users and requires minimal administrator configuration.

By automatically determining when users have logged in or out based on workstation IP address traffic, SonicWALL SSO is secure and hands-free. SSO authentication is designed to operate with any external agent that can return the identity of a user at a specific IP address using a SonicWALL ADConnector-compatible protocol.

SonicWALL SSO works for any service on the SonicWALL security appliances that uses user-level authentication, including Content Filtering Service (CFS), Firewall Access Rules, group membership and inheritance, and security services (IPS, GAV, SPY and Application Firewall) inclusion/exclusion lists.

Other benefits of SonicWALL SSO include:

- Ease of use — Users only need to sign in once to gain automatic access to multiple resources.
- Improved user experience — Windows domain credentials can be used to authenticate a user for any traffic type without logging in using a Web browser.
- Transparency to users — Users are not required to re-enter user name and password for authentication.
- Secure communication — Shared key encryption for data transmission protection.
- SonicWALL SSO Agent can be installed on any workstation on the LAN.
- Login mechanism works with any protocol, not just HTTP.

## Platforms

SSO is available on SonicWALL security appliances running SonicOS 4.0 Enhanced.

## Supported Standards

The SonicOS Enhanced 4.0 SSO feature supports LDAP and local database protocols.

To use SonicWALL SSO, it is required that the SonicWALL SSO Agent be installed on the workstations within your Windows domain that can reach clients directly using a static IP or through a VPN path. The following requirements must be met in order to run the SSO Agent:

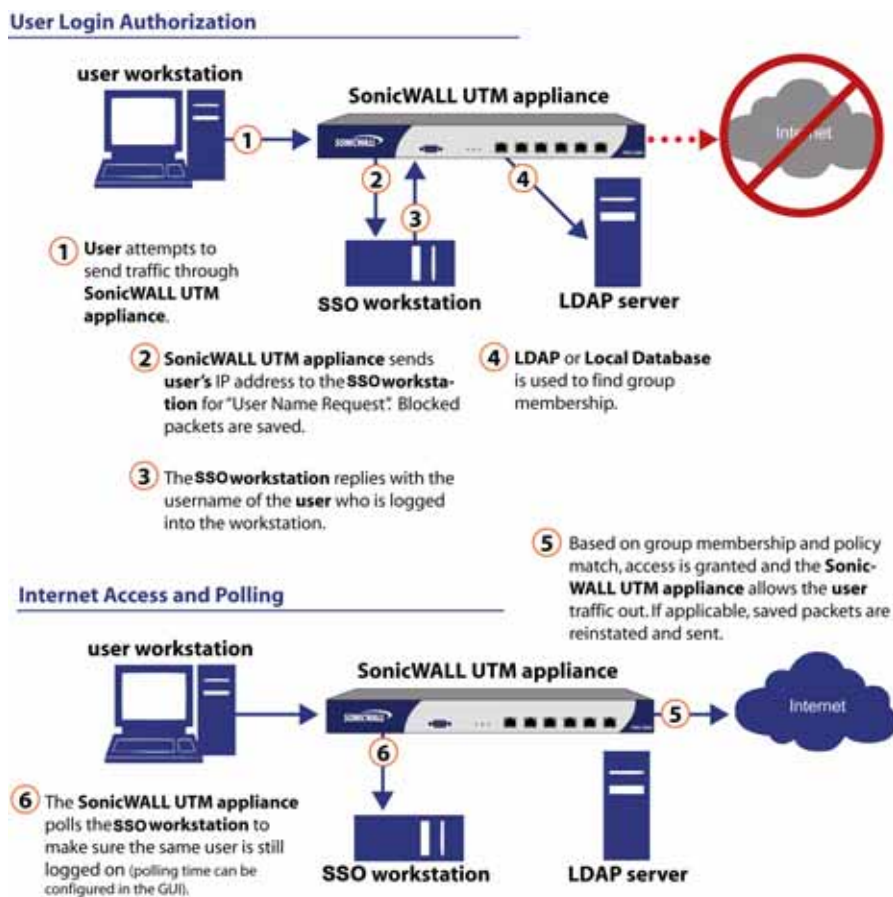
- Port 2258 must be open; the firewall uses UDP port 2258 by default to communicate with SonicWALL SSO Agent
- Windows 32 or XP, with latest service pack
- .NET Framework 2.0

- Net API or WMI

## How Does Single Sign-On Work?

SonicWALL SSO requires minimal administrator configuration and is transparent to the user. There are six steps involved in SonicWALL SSO authentication, as illustrated in [Figure 52:5](#).

**Figure 52:5 SonicWALL Single Sign-On Process**



The SonicWALL SSO authentication process is initiated when user traffic passes through a SonicWALL security appliance, for example, when a user accesses the Internet. The sent packets are temporarily blocked and saved while the SonicWALL security appliance sends a "User Name" request and workstation IP address to the authorization agent running the SSO Agent.

The authorization agent running the SSO Agent provides the SonicWALL security appliance with the username currently logged into the workstation. A User IP Table entry is created for the logged in user, similar to RADIUS and LDAP.

Once a user has been identified, the SonicWALL security appliance queries LDAP or a local database (based on administrator configuration) to find user group memberships, match the memberships against policy, and grant or restrict access to the user accordingly. Upon successful completion of the login sequence, the saved packets are sent on. If packets are received from the same source address before the sequence is completed, only the most recent packet will be saved.

User names are returned from the authorization agent running the SSO Agent in the format <domain>/<user-name>. For locally configured user groups, the user name can be configured to be the full name returned from the authorization agent running the SSO Agent (configuring the names in the SonicWALL security appliance local user database to match) or a simple user name with the domain component stripped off (default).

For the LDAP protocol, the <domain>/<user-name> format is converted to an LDAP distinguished name by creating an LDAP search for an object of class "domain" with a "dc" (domain component) attribute that matches the domain name. If one is found, then its distinguished name will be used as the directory sub-tree to search for the user's object. For example, if the user name is returned as "SV/bob" then a search for an object with "objectClass=domain" and "dc=SV" will be performed. If that returns an object with distinguished name "dc=sv,dc=us,dc=sonicwall,dc=com," then a search under that directory sub-tree will be created for (in the Active Directory case) an object with "objectClass=user" and "sAMAccountName=bob". If no domain object is found, then the search for the user object will be made from the top of the directory tree.

Once a domain object has been found, the information is saved to avoid searching for the same object. If an attempt to locate a user in a saved domain fails, the saved domain information will be deleted and another search for the domain object will be made.

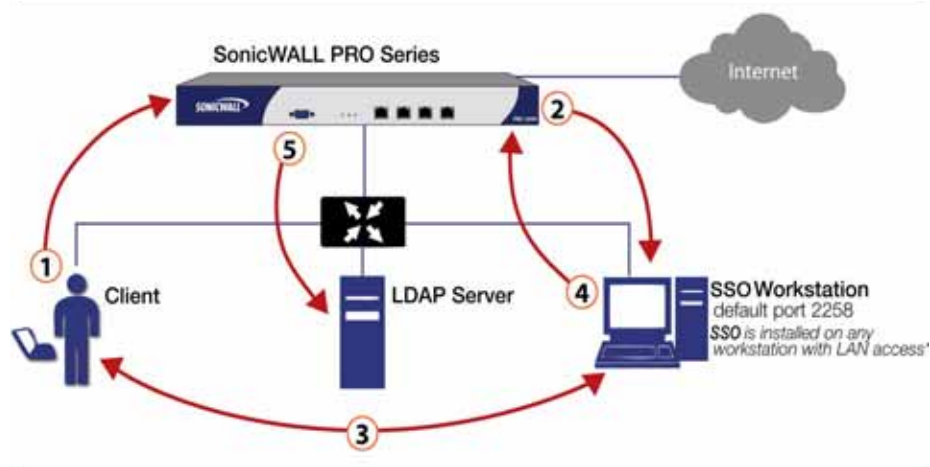
The SonicWALL security appliance polls the authorization agent running the SSO Agent at a configurable rate to determine when a user has logged out. Configurable user session limits, inactivity timers, and user name request polls are other methods to determine user logout status. Upon user logout, the authentication agent running the SSO Agent sends a User Logged Out response to the SonicWALL security appliance, confirming the user has been logged out and terminating the SSO session.

### **How Does SonicWALL SSO Agent Work?**

The SonicWALL SSO Agent can be installed on any workstation with a Windows domain that can communicate with clients and the SonicWALL security appliance directly using the IP address or using a path, such as VPN. For installation instructions for the SonicWALL SSO Agent, refer to the ["Installing the SonicWALL SSO Agent" section on page 643](#). The SonicWALL SSO Agent only communicates with clients and the SonicWALL security appliance. SonicWALL SSO Agent uses a shared key for encryption of messages between the SSO Agent and the SonicWALL security appliance. The shared key is generated in the SSO Agent and the key entered in the SonicWALL security appliance during SSO configuration must match the SSO Agent-generated key exactly.



Figure 52:6 SonicWALL SSO Agent Process



- 1 A client logs into the network and attempts to access the Internet or other network resources.
- 2 The SonicWALL security appliance queries the SonicWALL SSO (default port 2258) for the client ID.
- 3 The SonicWALL SSO passes on the request to the client and the client responds with its client ID.
- 4 Client ID information is passed back from the SonicWALL SSO to the SonicWALL security appliance.
- 5 Based on the client ID, the SonicWALL security appliance checks with the LDAP server to determine group membership and permissions.

Steps 2 3 4

Communication in these steps (between the SSO and client / firewall) is encrypted using a shared key which is generated by the SonicWALL SSO.

The SonicWALL security appliance queries the SonicWALL SSO Agent over the default port 2258. The SSO Agent then communicates between the client and the SonicWALL security appliance to determine the client's user ID. The SonicWALL SSO Agent is polled, at a rate that is configurable by the administrator, by the SonicWALL security appliance to continually confirm a user's login status.

## Logging

The SonicWALL SSO Agent sends log event messages to the Windows Event Log based on administrator-selected logging levels.

The SonicWALL security appliance also logs SSO Agent-specific events in its event log. The following is a list of SSO Agent-specific log event messages from the SonicWALL security appliance:

- **User login denied - not allowed by policy rule:** The user has been identified and does not belong to any user groups allowed by the policy blocking the user's traffic.
- **User login denied - not found locally:** The user has not been found locally, and Allow only users listed locally is selected in the SonicWALL security appliance.
- **User login denied - SSO Agent agent timeout:** Attempts to contact the SonicWALL SSO Agent have timed out.
- **User login denied - SSO Agent configuration error:** The SSO Agent is not properly configured to allow access for this user.
- **User login denied - SSO Agent communication problem:** There is a problem communicating with the workstation running the SonicWALL SSO Agent.

- User login denied - SSO Agent agent name resolution failed: The SonicWALL SSO Agent is unable to resolve the user name.
- **SSO Agent returned user name too long:** The user name is too long.
- SSO Agent returned domain name too long: The domain name is too long.

**Note**

The notes field of log messages specific to the SSO Agent will contain the text **<domain/user-name>, authentication by SSO Agent.**

## Multiple Administrator Support Overview

This section provides an introduction to the Multiple Administrators feature. This section contains the following subsections:

- [“What is Multiple Administrators Support?” section on page 610](#)
- [“Benefits” section on page 610](#)
- [“How Does Multiple Administrators Support Work?” section on page 610](#)

### What is Multiple Administrators Support?

The original version of SonicOS Enhanced supported only a single administrator to log on to a SonicWALL security appliance with full administrative privileges. Additional users can be granted “limited administrator” access, but only one administrator can have full access to modify all areas of the SonicOS GUI at one time.

SonicOS Enhanced release 4.0 introduces support for multiple concurrent administrators. This feature allows for multiple users to log-in with full administrator privileges. In addition to using the default **admin** user name, additional administrator usernames can be created.

Because of the potential for conflicts caused by multiple administrators making configuration changes at the same time, only one administrator is allowed to make configuration changes. The additional administrators are given full access to the GUI, but they cannot make configuration changes.

A number of options can be configured to manage multiple administrators on the **System > Administration** page. See the [“Multiple Administrators” section on page 76](#) for more information.

### Benefits

Multiple Administrators Support provides the following benefits:

- **Improved productivity** - Allowing multiple administrators to access a SonicWALL security appliance simultaneously eliminates “auto logout,” a situation that occurs when two administrators require access to the appliance at the same time and one is automatically forced out of the system.
- **Reduced configuration risk** – The new read-only mode allows users to view the current configuration and status of a SonicWALL security appliance without the risk of making unintentional changes to the configuration.

### How Does Multiple Administrators Support Work?

The following sections describe how the Multiple Administrators Support feature works:

- [“Configuration Modes” section on page 611](#)

- “User Groups” section on page 612
- “Priority for Preempting Administrators” section on page 612
- “GMS and Multiple Administrator Support” section on page 613

### Configuration Modes

In order to allow multiple concurrent administrators, while also preventing potential conflicts caused by multiple administrators making configuration changes at the same time, the following configuration modes have been defined:

- **Configuration mode** - Administrator has full privileges to edit the configuration. If no administrator is already logged into the appliance, this is the default behavior for administrators with full and limited administrator privileges (but not read-only administrators).



**Note**

Administrators with full configuration privilege can also log in using the Command Line Interface (CLI).

- **Read-only mode** - Administrator cannot make any changes to the configuration, but can view the browse the entire management UI and perform monitoring actions.

Only administrators that are members of the **SonicWALL Read-Only Admins** user group are given read-only access, and it is the only configuration mode they can access.

- **Non-configuration mode** - Administrator can view the same information as members of the read-only group and they can also initiate management actions that do not have the potential to cause configuration conflicts.

Only administrators that are members of the **SonicWALL Administrators** user group can access non-configuration mode. This mode can be entered when another administrator is already in configuration mode and the new administrator chooses not to preempt the existing administrator. By default, when an administrator is preempted out of configuration mode, he or she is converted to non-configuration mode. On the **System > Administration** page, this behavior can be modified so that the original administrator is logged out.

The following table provides a summary of the access rights available to the configuration modes. Access rights for limited administrators are included also, but note that this table does not include all functions available to limited administrators.

Function	Full admin in config mode	Full admin in non-config mode	Read-only administrator	Limited administrator
Import certificates	X			
Generate certificate signing requests	X			
Export certificates	X			
Export appliance settings	X	X	X	
Download TSR	X	X	X	
Use other diagnostics	X	X		X
Configure network	X			X
Flush ARP cache	X	X		X
Setup DHCP Server	X			

Function	Full admin in config mode	Full admin in non-config mode	Read-only administrator	Limited administrator
Renegotiate VPN tunnels	X	X		
Log users off	X	X		X guest users only
Unlock locked-out users	X	X		
Clear log	X	X		X
Filter logs	X	X	X	X
Export log	X	X	X	X
Email log	X	X		X
Configure log categories	X	X		X
Configure log settings	X			X
Generate log reports	X	X		X
Browse the full UI	X	X	X	
Generate log reports	X	X		X

### User Groups

The Multiple Administrators Support feature introduces two new default user groups:

- **SonicWALL Administrators** - Members of this group have full administrator access to edit the configuration.
- **SonicWALL Read-Only Admins** - Members of this group have read-only access to view the full management interface, but they cannot edit the configuration and they cannot switch to full configuration mode.

It is not recommended to include users in more than one of these user groups. However, if you do so, the following behavior applies:

- If members of the **SonicWALL Administrators** user group are also included in the **Limited Administrators** or **SonicWALL Read-Only Admins** user groups, the members will have full administrator rights.
- If members of the **Limited Administrators** user group are included in the **SonicWALL Read-Only Admins** user group, the members will have limited administrator rights.

### Priority for Preempting Administrators

The following rules govern the priority levels that the various classes of administrators have for preempting administrators that are already logged into the appliance:

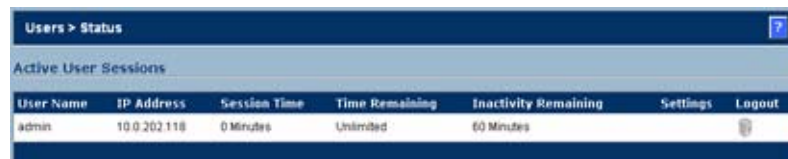
1. The **admin** user and SonicWALL Global Management System (GMS) both have the highest priority and can preempt any users.
2. A user that is a member of the **SonicWALL Administrators** user group can preempt any users except for the **admin** and SonicWALL GMS.
3. A user that is a member of the **Limited Administrators** user group can only preempt other members of the **Limited Administrators** group.

### GMS and Multiple Administrator Support


When using SonicWALL GMS to manage a SonicWALL security appliance, GMS frequently logs in to the appliance (for such activities as ensuring that GMS management IPsec tunnels have been created correctly). These frequent GMS log-ins can make local administration of the appliance difficult because the local administrator can be preempted by GMS.

## Viewing Status on Users > Status

The **Users > Status** page displays **Active User Sessions** on the SonicWALL. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. To log a user out, click the Trashcan icon next to the user's entry.



The screenshot shows the 'Users > Status' page with a table of active user sessions. The table has columns for User Name, IP Address, Session Time, Time Remaining, Inactivity Remaining, Settings, and Logout. A single entry for 'admin' is shown with IP 10.0.202.118, 0 Minutes session time, Unlimited time remaining, and 60 Minutes inactivity remaining. A trashcan icon is visible in the Logout column for the admin user.

User Name	IP Address	Session Time	Time Remaining	Inactivity Remaining	Settings	Logout
admin	10.0.202.118	0 Minutes	Unlimited	60 Minutes		

## Configuring Settings on Users > Settings

On this page, you can configure the authentication method required, global user settings, and an acceptable user policy that is displayed to users when logging onto your network.

**Users > Settings** [Apply] [Cancel] [?]

**User Login Settings**

Authentication method for login: Local Users [Configure...]

Single-sign-on method: SonicWALL SSD Agent [Configure...]

Show authentication page for (minutes): 1 [?]

Case-sensitive user names

Enforce login uniqueness

Redirect users from HTTPS to HTTP on completion of login

**User Session Settings**

Inactivity timeout (minutes): 15

Enable login session limit

Login session limit (minutes): 30

Show user login status window [?]

User's login status window sends heartbeat every (seconds): 120

Enable disconnected user detection

Timeout on heartbeat from user's login status window (minutes): 10

**Other Global User Settings**

Allow these HTTP URLs to bypass user authentication in access rules:

None

[Add] [Remove]

**Acceptable Use Policy**

Display on login from:  Trusted Zones  WAN Zone  Public Zones  Wireless Zones  VPN Zone

Window size (pixels): 460 x 310

Enable scroll bars on the window

Acceptable use policy page content:

[Example Template] [Preview...]

Note: Acceptable use policy text may include HTML formatting.

Configuration instructions for the settings on this page are provided in the following sections:

- “User Login Settings” on page 615
- “User Session Settings” on page 616
- “Other Global User Settings” on page 617
- “Acceptable Use Policy” on page 617

## User Login Settings

In the **Authentication method for login** drop-down list, select the type of user account management your network uses:

- Select **Local Users** to configure users in the local database in the SonicWALL appliance using the **Users > Local Users** and **Users > Local Groups** pages.

For information about using the local database for authentication, see [“Using Local Users and Groups for Authentication” on page 600](#).

For detailed configuration instructions, see the following sections:

- “Configuring Local Users” on page 618
- “Configuring Local Groups” on page 621

- Select **RADIUS** if you have more than 1,000 users or want to add an extra layer of security for authenticating the user to the SonicWALL. If you select RADIUS for user authentication, users must log into the SonicWALL using HTTPS in order to encrypt the password sent to the SonicWALL. If a user attempts to log into the SonicWALL using HTTP, the browser is automatically redirected to HTTPS.

For information about using the local database for authentication, see [“Using RADIUS for Authentication” on page 602](#).

For detailed configuration instructions, see [“Configuring RADIUS Authentication” on page 625](#)

- Select **RADIUS + Local Users** if you want to use both RADIUS and the SonicWALL local user database for authentication.
- Select **LDAP** if you use a Lightweight Directory Access Protocol (LDAP) server, Microsoft Active Directory (AD) server, or Novell eDirectory to maintain all your user account data.

For information about using the local database for authentication, see [“Using LDAP / Active Directory / eDirectory Authentication” on page 602](#).

For detailed configuration instructions, see [“Configuring LDAP Integration in SonicOS Enhanced” on page 631](#)

- Select **LDAP + Local Users** if you want to use both LDAP and the SonicWALL local user database for authentication.

In the **Single-sign-on method** drop-down list, select **SonicWALL SSO Agent** if you are using Active Directory for authentication and the SonicWALL SSO Agent is installed on a computer in the same domain. Otherwise, select **None**. For detailed SSO configuration instructions, see [“Configuring Single Sign-On” on page 641](#).

In the **Show user authentication page for** field, enter the number of minutes that a user has to log in before the login page times out. If it times out, a message displays saying they must click before attempting to log in again.



A screenshot of the SonicWALL login interface. It features a blue background with two white input fields labeled 'Name' and 'Password'. Below the 'Password' field is a blue 'Login' button.



Select **Case-sensitive user names** to enable matching based on capitalization of user account names.

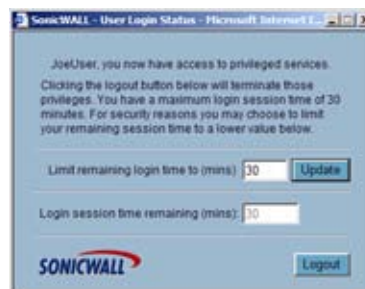
Select **Enforce login uniqueness** to prevent the same user name from being used to log into the network from more than one location at a time. This setting applies to both local users and RADIUS/LDAP users. However the login uniqueness setting does not apply to the default administrator with the username **admin**.

Select **Redirect users from HTTPS to HTTP on completion of login** if you want users to be connected to the network through your SonicWALL appliance via HTTP after logging in via HTTPS. If you have a large number of users logging in via HTTPS, you may want to redirect them to HTTP, because HTTPS consumes more system resources than HTTP. If you deselect this option, you will see a warning dialog.

## User Session Settings

The settings listed below apply to all users when authenticated through the SonicWALL.

- **Inactivity timeout (minutes):** users can be logged out of the SonicWALL after a preconfigured inactivity time. Enter the number of minutes in this field. The default value is **5** minutes.
- **Enable login session limit:** you can limit the time a user is logged into the SonicWALL by selecting the check box and typing the amount of time, in minutes, in the **Login session limit (minutes)** field. The default value is **30** minutes.
- **Show user login status window:** causes a status window to display with a **Log Out** button during the user's session. The user can click the **Log Out** button to log out of their session.



The **User Login Status** window displays the number of minutes the user has left in the login session. The user can set the remaining time to a smaller number of minutes by entering the number and clicking the **Update** button.

If the user is a member of the Limited Administrators user group, the **User Login Status** window has a **Manage** button the user can click to automatically log into the SonicWALL appliance's management interface. See ["Configuring Local Groups"](#) on page 621 for information on the Limited Administrators group.



- **User's login status window sends heartbeat every (seconds):** Sets the frequency of the heartbeat signal used to detect whether the user still has a valid connection



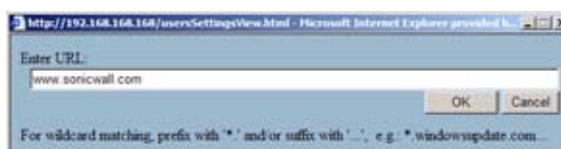
- **Enable disconnected user detection:** Causes the SonicWALL to detect when a user's connection is no longer valid and end the session.
- **Timeout on heartbeat from user's login status window (minutes):** Sets the time needed without a reply from the heartbeat before ending the user session.

## Other Global User Settings

- **Allow these HTTP URLs to bypass users authentication access rules:** Define a list of URLs users can connect to without authenticating. To add a URL to the list:

**Step 1** Click **Add** below the URL list.

**Step 2** In the **Enter URL** window, enter the top level URL you are adding, for example, `www.sonicwall.com`. All sub directories of that URL are included, such as `www.sonicwall.com/us/Support.html`. Click on **OK** to add the URL to the list.



## Acceptable Use Policy

An acceptable use policy (AUP) is a policy that users must agree to follow in order to access a network or the Internet. It is common practice for many businesses and educational facilities to require that employees or students agree to an acceptable use policy before accessing the network or Internet through the SonicWALL.

The **Acceptable Use Policy** section allows you to create the AUP message window for users. You can use HTML formatting in the body of your message. Clicking the **Example Template** button creates a preformatted HTML template for your AUP window.

- **Display on login from** - Select the network interface(s) you want to display the Acceptable Use Policy page when users login. You can choose **Trusted Zones**, **WAN Zone**, **Public Zones**, **Wireless Zones**, and **VPN Zone** in any combination.
- **Window size (pixels)** - Allows you to specify the size of the AUP window defined in pixels. Checking the **Enable scroll bars on the window** allows the user to scroll through the AUP window contents.
- **Enable scroll bars on window** - Turns on the scroll bars if your content will exceed the display size of the window.

**Acceptable use policy** page content - Enter your Acceptable Use Policy text in the text box. You can include HTML formatting. The page that is displayed to the user includes an **I Accept** button or **Cancel** button for user confirmation.



Click the **Example Template** button to populate the content with the default AUP template, which you can modify:

```
<font face=arial size=3>
<center><b><i>Welcome to the SonicWALL</i></b></center></b></i>
<font size=2>

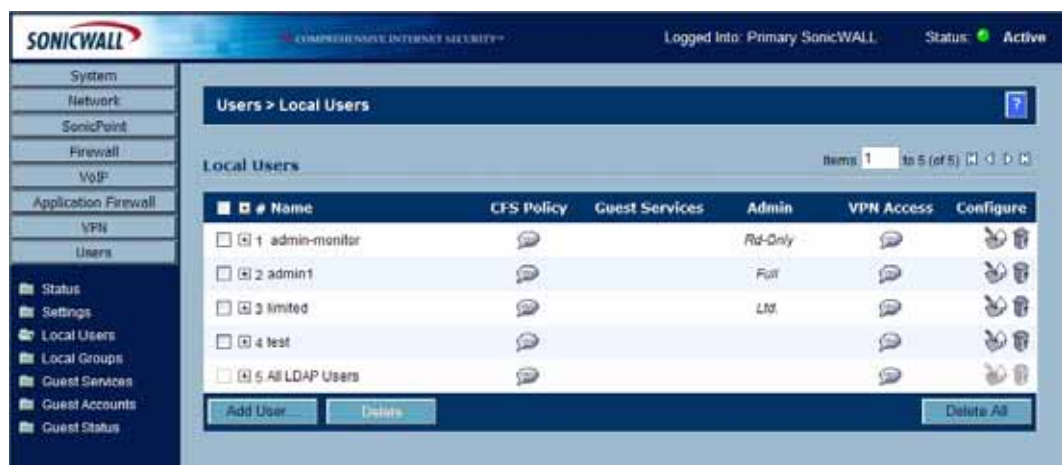
<table width="100%" border="1">
<tr><td>
<font size=2>
<br><br><br>
<center>Enter your usage policy terms here.
<br><br><br>
</td></tr>
</table>
```

Click "I Accept" only if you wish to accept these terms and continue, or otherwise select "Cancel".

Click the **Preview** button to display your AUP message as it will appear for the user.

## Configuring Local Users


Local Users are users stored and managed on the security appliance's local database. In the **Users > Local Users** page, you can view and manage all local users, add new local users, and edit existing local users.



See the following sections for configuration instructions:

- “Viewing, Editing and Deleting Local Users” on page 619
- “Adding Local Users” on page 620
- “Editing Local Users” on page 621





## Viewing, Editing and Deleting Local Users

You can view all the groups to which a user belongs on the **Users > Local Users** page. Click on the expand icon  next to a user to view the group memberships for that user.



#	Name	CFS Policy	Guest Services	Limited Admin	VPN Access	Configure
1	JoeUser		<input checked="" type="checkbox"/>			
2	SueUser		<input checked="" type="checkbox"/>			
	Everyone					
	Guest Services		<input checked="" type="checkbox"/>			
	Trusted Users					
3	EleanorEland		<input checked="" type="checkbox"/>			
4	LarryLagarto	Filters bypassed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
5	HiramMyrae					

The three columns to the right of the user's name list the privileges that the user has. In the expanded view, it displays which group the user gets each privilege from.

- Hover the mouse pointer over the comment icon  in the VPN Access column to view the network resources to which the user has VPN access.
- In the expanded view, click the remove icon  under Configure to remove the user from a group.
- Click the edit icon  under Configure to edit the user.
- Click the delete icon  under Configure to delete the user or group in that row.

## Adding Local Users

You can add local users to the internal database on the SonicWALL security appliance from the **Users > Local Users** page. To add local users to the database:

**Step 1** Click **Add User**. The **Add User** configuration window displays.

The screenshot shows the 'Add User' configuration window with the following fields and values:

- Name:** test
- Password:** [masked]
- Confirm Password:** [masked]
- User must change password:**
- Comment:** this is a test

Buttons: OK, Cancel

**Step 2** On the **Settings** tab, type the user name into the **Name** field.

**Step 3** In the **Password** field, type a password for the user. Passwords are case-sensitive and should consist of a combination of letters and numbers rather than names of family, friends, or pets.

**Step 4** Confirm the password by retyping it in the **Confirm Password** field.

**Step 5** Optionally, select the **User must change password** checkbox to force users to change their passwords the first time they login.

**Step 6** Optionally enter a comment in the **Comment** field.

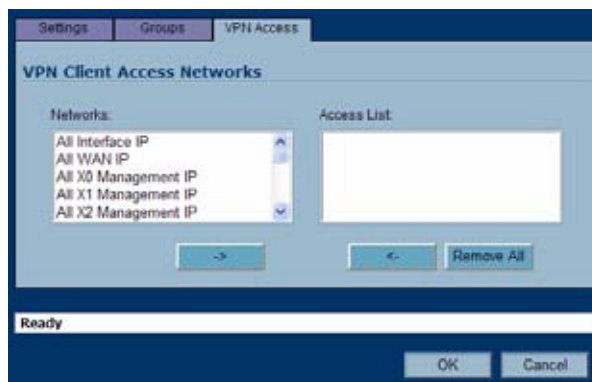
**Step 7** On the **Groups** tab, under **User Groups**, select one or more groups to which the user will belong, and click the arrow button -> to move the group name(s) into the **Member of** list. The user will be a member of the selected groups. To remove the user from a group, select the group from the **Member of** list, and click the left arrow button <-.

The screenshot shows the 'Group Memberships' configuration window with the following elements:

- User Groups:** Content Filtering Bypass, Guest Services, Limited Administrators, SonicWALL Administrators, SonicWALL Read-Only Admins
- Member Of:** Everyone, Trusted Users
- Buttons:** Add All, ->, <-, Remove All

Buttons: OK, Cancel

**Step 8** On the **VPN Access** tab, to allow users to access networks using a VPN tunnel, select one or more networks from the **Networks** list and click the arrow button -> to move them to the **Access List**. To remove the user's access to a network, select the network from the **Access List**, and click the left arrow button <-.



**Step 9** Click **OK** to complete the user configuration.

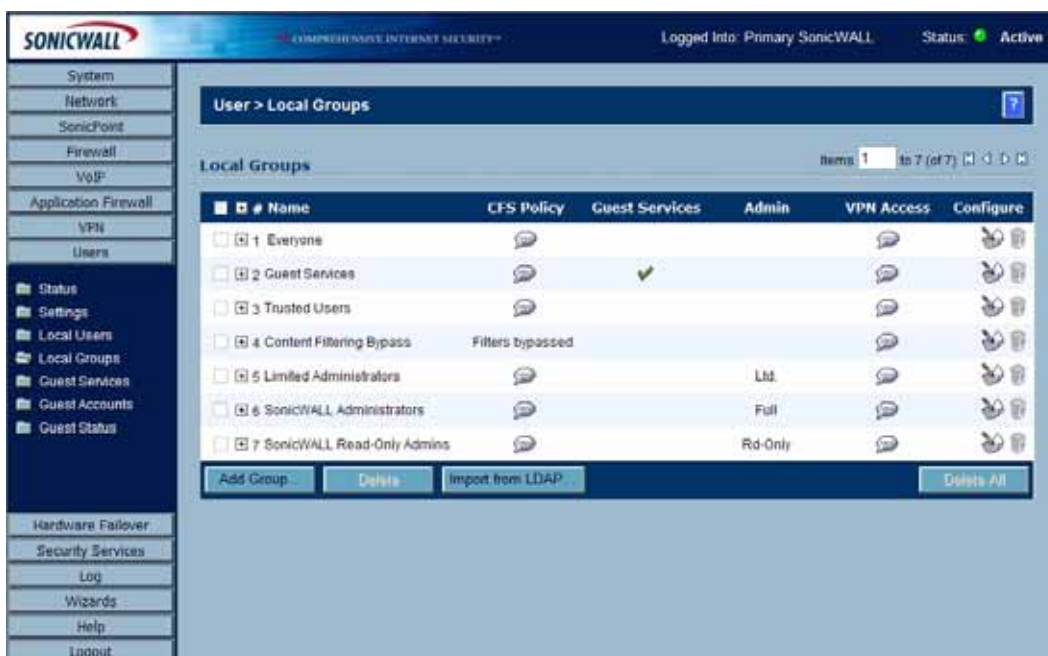
## Editing Local Users

You can edit local users from the **Users > Local Users** screen. To edit a local user:

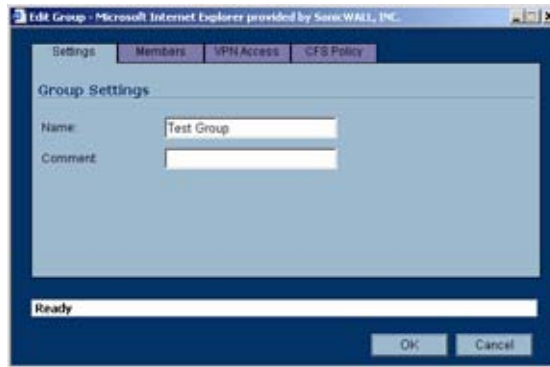
- Step 1** In the list of users, click the edit icon in same line as the user you want to edit.
- Step 2** Configure the **Settings**, **Groups**, and **VPN Access** exactly as when adding a new user. See [“Adding Local Users” on page 620](#).

## Configuring Local Groups

Local groups are displayed in the **Local Groups** table. The table lists **Name**, **CFS Policy**, **Guest Services**, **Admin** (access type), **VPN Access**, and **Configure**.



A default group, **Everyone**, is listed in the first row of the table. Click the Notepad icon in the **Configure** column to review or change the settings for **Everyone**.

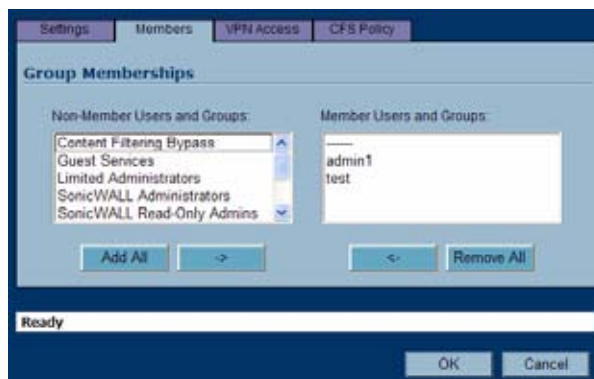


See the following sections for configuration instructions:

- “Creating a Local Group” on page 623
- “Importing Local Groups from LDAP” on page 624

## Creating a Local Group

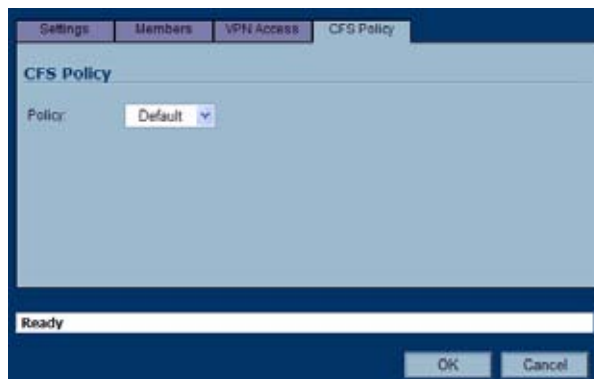
- Step 1** Click the **Add Group** button to display the **Add Group** window.
- Step 2** On the **Settings** tab, type a user name into the **Name** field.
- Step 3** On the **Members** tab, to add users and other groups to this group, select the user or group from the **Non-Members Users and Groups** list and click the right arrow button ->.



- Step 4** On the **VPN Access** tab, to allow users in this group to access networks using a VPN tunnel, select the networks from the **Networks** list and click the right arrow button -> to move them to the **Access List**.



- Step 5** On the **CFS Policy** tab, to enforce a custom Content Filtering Service policy for this group, select the CFS policy from the **Policy** drop-down list.



**Note**

You can create custom Content Filtering Service policies in the **Security Services > Content Filter** page. See [“Security Services > Content Filter”](#) section on page 695.

**Step 6** Click **OK**.

## Importing Local Groups from LDAP

You can configure local user groups on the SonicWALL by retrieving the user group names from your LDAP server. The **Import from LDAP...** button launches a dialog box containing the list of user group names available for import to the SonicWALL.

Having user groups on the SonicWALL with the same name as existing LDAP/AD user groups allows SonicWALL group memberships and privileges to be granted upon successful LDAP authentication.

To import groups from the LDAP server:

**Step 1** In the **Users > Local Groups** page, click **Import from LDAP...**

#	Name	CFS Policy	Guest Services	Admin	VPN Access	Configure
1	Everyone					
2	Guest Services		✓			
3	Trusted Users					
4	Content Filtering Bypass	Filters bypassed				
5	Limited Administrators			Ltd.		
6	SonicWALL Administrators			Full		
7	SonicWALL Read-Only Admins			Rd-Only		

**Step 2** In the **LDAP Import User Groups** dialog box, select the checkbox for each group that you want to import into the SonicWALL, and then click **Save**.



## Configuring RADIUS Authentication

If you selected **RADIUS** or **RADIUS + Local Users** from the **Authentication method for login** drop-down list, the **Configure** button becomes available.

- Step 1** Click **Configure** to set up your RADIUS server settings on the SonicWALL. The **RADIUS Configuration** window is displayed.

The screenshot shows the 'RADIUS Configuration' window with the following fields and values:

- Global RADIUS Settings:**
  - RADIUS Server Timeout (seconds): 5
  - Retries: 3
- RADIUS Servers:**
  - Primary Server:**
    - Name or IP Address: [Empty]
    - Shared Secret: [Empty]
    - Port Number: 1812
  - Secondary Server:**
    - Name or IP Address: [Empty]
    - Shared Secret: [Empty]
    - Port Number: 1812

- Step 2** Under **Global RADIUS Settings**, type in a value for the **RADIUS Server Timeout (seconds)**. The allowable range is 1-60 seconds with a default value of 5.
- Step 3** In the **Retries** field, enter the number of times the SonicWALL will attempt to contact the RADIUS server. If the RADIUS server does not respond within the specified number of retries, the connection is dropped. This field can range between 0 and 10, with a recommended setting of 3 RADIUS server retries.

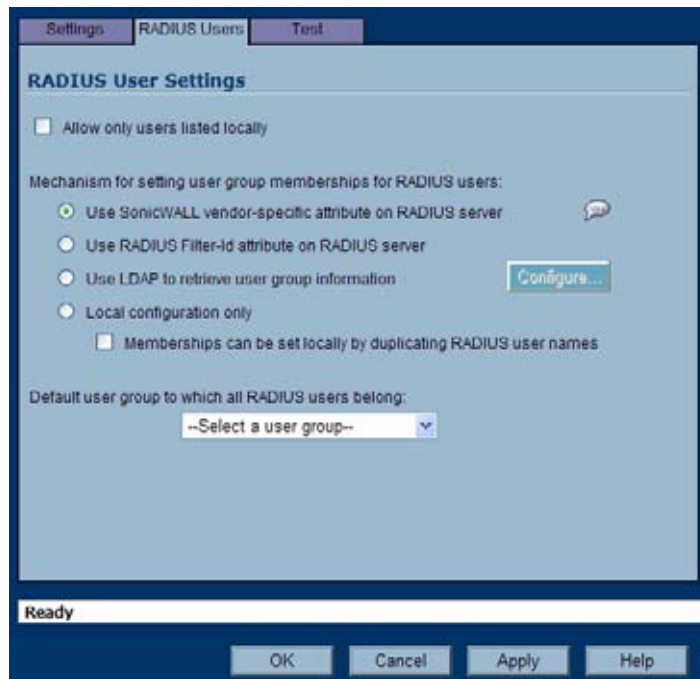
## RADIUS Servers

In the **RADIUS Servers** section, you can designate the primary and optionally, the secondary RADIUS server. An optional secondary RADIUS server can be defined if a backup RADIUS server exists on the network.

- Step 4** In the **Primary Server** section, type the host name or IP address of the RADIUS server in the **Name or IP Address** field.
- Step 5** Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
- Step 6** Type the **Port Number** for the RADIUS server to use for communication with the SonicWALL. The default is 1812.
- Step 7** In the **Secondary Server** section, optionally type the host name or IP address of the secondary RADIUS server in the **Name or IP Address** field.
- Step 8** Type the RADIUS server administrative password or “shared secret” in the **Shared Secret** field. The alphanumeric **Shared Secret** can range from 1 to 31 characters in length. The shared secret is case sensitive.
- Step 9** Type the **Port Number** for the secondary RADIUS server to use for communication with the SonicWALL. The default is 1812.

## RADIUS Users

On the **RADIUS Users** tab you can specify what types of local or LDAP information to use in combination with RADIUS authentication. You can also define the default user group for RADIUS users.



## RADIUS Users Settings

To configure the RADIUS user settings:

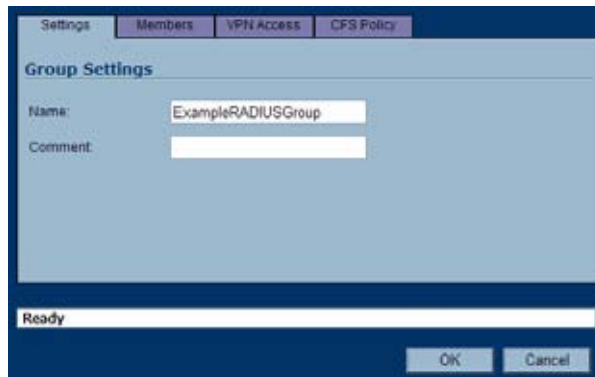
- Step 10** On the **RADIUS Users** tab, select **Allow only users listed locally** if only the users listed in the SonicWALL database are authenticated using RADIUS.
- Step 11** Select the mechanism used for setting user group memberships for RADIUS users from the following choices:
- Select **Use SonicWALL vendor-specific attribute on RADIUS server** to apply a configured vendor-specific attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
  - Select **Use RADIUS Filter-ID attribute on RADIUS server** to apply a configured Filter-ID attribute from the RADIUS server. The attribute must provide the user group to which the user belongs.
  - Select **Use LDAP to retrieve user group information** to obtain the user group from the LDAP server. You can click the Configure button to set up LDAP if you have not already configured it or if you need to make a change. For information about configuring LDAP, see “Configuring the SonicWALL Appliance for LDAP” on page 633.
  - If you do not plan to retrieve user group information from RADIUS or LDAP, select **Local configuration only**.
  - For a shortcut for managing RADIUS user groups, check **Memberships can be set locally by duplicating RADIUS user names**. When you create users with the same name locally on the security appliance and manage their group memberships, the memberships in the RADIUS database will automatically change to mirror your local changes.
- Step 12** If you have previously configured User Groups on the SonicWALL, select the group from the **Default user group to which all RADIUS users belong** drop-down list.

## Creating a New User Group for RADIUS Users


In the RADIUS User Settings screen, you can create a new group by choosing **Create a new user group...** from the **Default user group to which all RADIUS users belong** drop-down list:

**Step 1** Select **Create a new user group...** The Add Group window displays.

**Step 2** In the **Settings** tab, enter a name for the group. You may enter a descriptive comment as well.



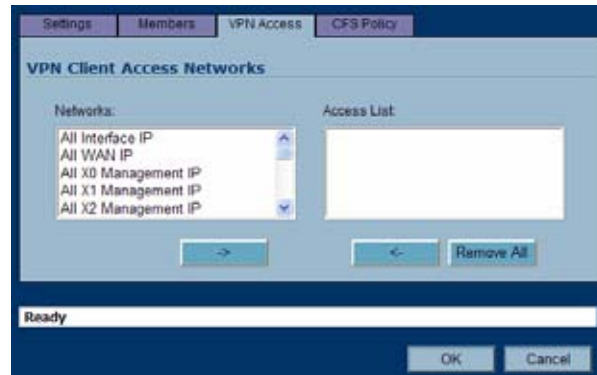
**Step 3** In the **Members** tab, select the members of the group. Select the users or groups you want to add in the left column and click the **->** button. Click **Add All** to add all users and groups.



**Note**

You can add any group as a member of another group except **Everybody** and **All RADIUS Users**. Be aware of the membership of the groups you add as members of another group.

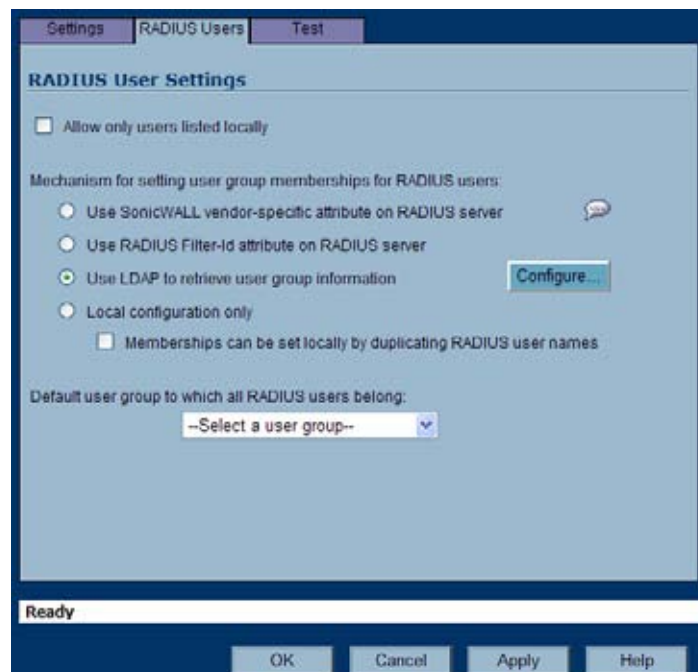
- Step 4** In the **VPN Access** tab, select the network resources to which this group will have VPN Access by default.



- Step 5** If you have Content Filtering Service (CFS) on your security appliance, you can configure the content filtering policy for this group on the **CFS Policy** tab. See [“Security Services > Content Filter” section on page 695](#) for instructions on registering for and managing the SonicWALL Content Filtering Service.

## RADIUS with LDAP for user groups

When RADIUS is used for user authentication, there is an option on the RADIUS Users page in the RADIUS configuration to allow LDAP to be selected as the mechanism for setting user group memberships for RADIUS users:



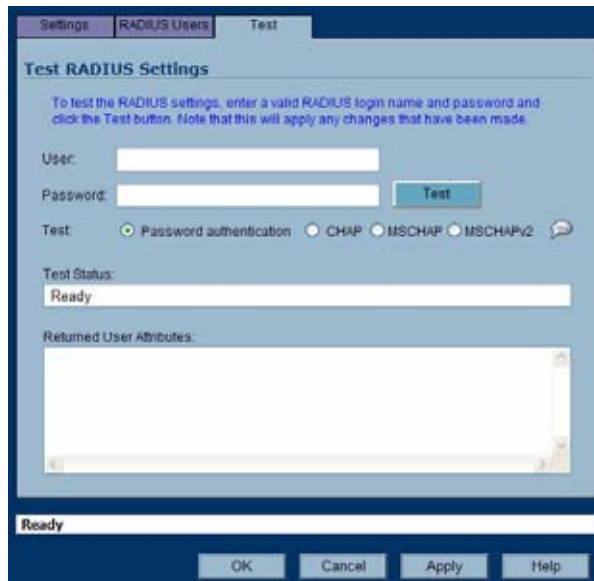
When **Use LDAP to retrieve user group information** is selected, after authenticating a user via RADIUS, his/her user group membership information will be looked up via LDAP in the directory on the LDAP/AD server.

Clicking the **Configure** button launches the LDAP configuration window.

Note that in this case LDAP is not dealing with user passwords and the information that it reads from the directory is normally unrestricted, so operation without TLS could be selected, ignoring the warnings, if TLS is not available (e.g. if certificate services are not installed with Active Directory). However, it must be ensured that security is not compromised by the SonicWALL doing a clear-text login to the LDAP server – e.g. create a user account with read-only access to the directory dedicated for the SonicWALL's use. Do not use the administrator account in this case.

## RADIUS Client Test

In the RADIUS Configuration dialog box, you can test your RADIUS Client user name, password and other settings by typing in a valid user name and password and selecting one of the authentication choices for **Test**. Performing the test will apply any changes that you have made.



To test your RADIUS settings:

- Step 6** In the **User** field, type a valid RADIUS login name.
- Step 7** In the **Password** field, type the password.
- Step 8** For **Test**, select one of the following:
  - **Password authentication:** Select this to use the password for authentication.
  - **CHAP:** Select this to use the Challenge Handshake Authentication Protocol. After initial verification, CHAP periodically verifies the identity of the client by using a three-way handshake.
  - **MSCHAP:** Select this to use the Microsoft implementation of CHAP. MSCHAP works for all Windows versions before Windows Vista.

- **MSCHAPv2:** Select this to use the Microsoft version 2 implementation of CHAP. MSCHAPv2 works for Windows 2000 and later versions of Windows.

**Step 9** Click the **Test** button. If the validation is successful, the **Status** messages changes to **Success**. If the validation fails, the **Status** message changes to **Failure**.

To complete the RADIUS configuration, click **OK**.

Once the SonicWALL has been configured, a VPN Security Association requiring RADIUS authentication prompts incoming VPN clients to type a User Name and Password into a dialog box.

## Configuring LDAP Integration in SonicOS Enhanced

Integrating your SonicWALL appliance with an LDAP directory service requires configuring your LDAP server for certificate management, installing the correct certificate on your SonicWALL appliance, and configuring the SonicWALL appliance to use the information from the LDAP Server.

See the following sections:

- [“Preparing Your LDAP Server for Integration” on page 631](#)
- [“Configuring the SonicWALL Appliance for LDAP” on page 633](#)

### Preparing Your LDAP Server for Integration

Before beginning your LDAP configuration, you should prepare your LDAP server and your SonicWALL for LDAP over TLS support. This requires:

- Installing a server certificate on your LDAP server.
- Installing a CA (Certificate Authority) certificate for the issuing CA on your SonicWALL appliance.

The following procedures describe how to perform these tasks in an Active Directory environment.

#### Configuring the CA on the Active Directory Server

To configure the CA on the Active Directory server (skip the first five steps if Certificate Services are already installed):

- 
- Step 1** Navigate to **Start > Settings > Control Panel > Add/Remove Programs**
  - Step 2** Select **Add/Remove Windows Components**
  - Step 3** Select **Certificate Services**
  - Step 4** Select **Enterprise Root CA** when prompted.
  - Step 5** Enter the requested information. For information about certificates on Windows systems, see

<http://support.microsoft.com/kb/931125>.

- Step 6** Launch the **Domain Security Policy** application: Navigate to **Start > Run** and run the command: **dmpol.msc**.
- Step 7** Open **Security Settings > Public Key Policies**.
- Step 8** Right click **Automatic Certificate Request Settings**.
- Step 9** Select **New > Automatic Certificate Request**.
- Step 10** Step through the wizard, and select **Domain Controller** from the list.

### Exporting the CA Certificate from the Active Directory Server

To export the CA certificate from the AD server:

- 
- Step 1** Launch the **Certification Authority** application: **Start > Run > certsrv.msc**.
  - Step 2** Right click on the CA you created, and select **properties**.
  - Step 3** On the **General** tab, click the **View Certificate** button.
  - Step 4** On the **Details** tab, select **Copy to File**.
  - Step 5** Step through the wizard, and select the **Base-64 Encoded X.509 (.cer)** format.
  - Step 6** Specify a path and filename to which to save the certificate.

### Importing the CA Certificate onto the SonicWALL

To import the CA certificate onto the SonicWALL:

- 
- Step 1** Browse to **System > CA Certificates**.
  - Step 2** Select **Add new CA certificate**. Browse to and select the certificate file you just exported.
  - Step 3** Click the **Import certificate** button.



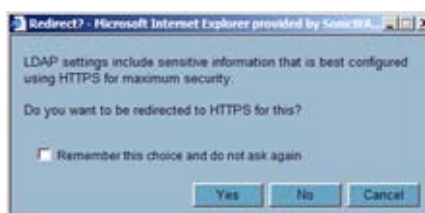
## Configuring the SonicWALL Appliance for LDAP

The **Users > Settings** page in the administrative interface provides the settings for managing your LDAP integration:

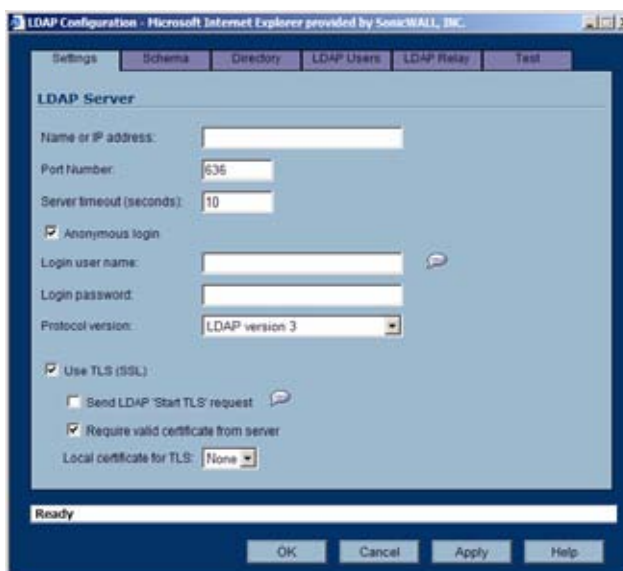
- Step 1** In the SonicOS administrative interface, open the **Users > Settings** page.
- Step 2** In the **Authentication method for login** drop-down list, select either **LDAP** or **LDAP + Local Users**.



- Step 3** Click **Configure**.
- Step 4** If you are connected to your SonicWALL appliance via HTTP rather than HTTPS, you will see a dialog box warning you of the sensitive nature of the information stored in directory services and offering to change your connection to HTTPS. If you have HTTPS management enabled for the interface to which you are connected (recommended), click **Yes**.



- Step 5** On the **Settings** tab of the LDAP Configuration window, configure the following fields:



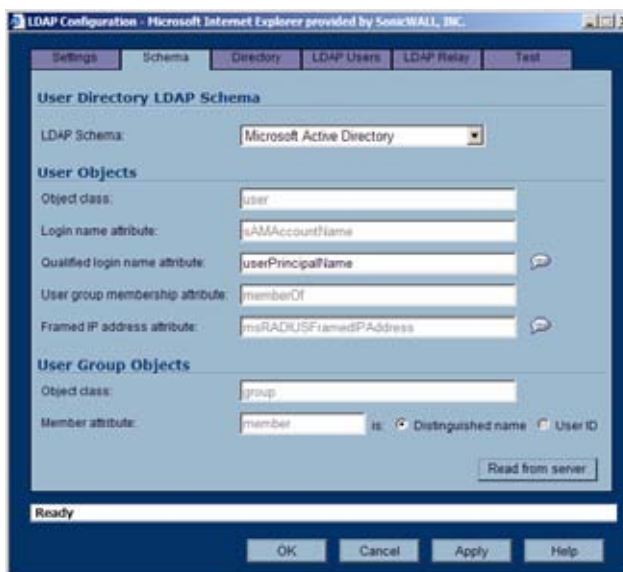
- **Name or IP Address** – The FQDN or the IP address of the LDAP server against which you wish to authenticate. If using a name, be certain that it can be resolved by your DNS server. Also, if using TLS with the 'Require valid certificate from server' option, the name provided here must match the name to which the server certificate was issued (i.e. the CN) or the TLS exchange will fail.

- **Port Number** – The default LDAP over TLS port number is TCP 636. The default LDAP (unencrypted) port number is TCP 389. If you are using a custom listening port on your LDAP server, specify it here.
- **Server timeout** – The amount of time, in seconds, that the SonicWALL will wait for a response from the LDAP server before timing out. Allowable ranges are 1 to 99999 (in case you're running your LDAP server on a VIC-20 located on the moon), with a default of 10 seconds.
- **Anonymous Login** – Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (Active Directory generally does not), then you may select this option.
- **Login user name** – Specify a user name that has rights to log in to the LDAP directory. The login name will automatically be presented to the LDAP server in full 'dn' notation. This can be any account with LDAP read privileges (essentially any user account) – Administrative privileges are not required. *Note that this is the user's name, not their login ID (e.g. John Smith rather than jsmith).*
- **Login password** – The password for the user account specified above.
- **Protocol version** – Select either LDAPv3 or LDAPv2. Most modern implementations of LDAP, including Active Directory, employ LDAPv3.
- **Use TLS** – Use Transport Layer Security (SSL) to log in to the LDAP server. It is strongly recommended that TLS be used to protect the username and password information that will be sent across the network. Most modern implementations of LDAP server, including Active Directory, support TLS. Deselecting this default setting will display an alert that you must accept to proceed.
- **Send LDAP 'Start TLS' Request** – Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. Active Directory does not use this option, and it should only be selected if required by your LDAP server.
- **Require valid certificate from server** – Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWALL and the LDAP server will still use TLS – only without issuance validation.
- **Local certificate for TLS** – Optional, to be used only if the LDAP server requires a client certificate for connections. Useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (Active Directory does not return passwords). This setting is not required for Active Directory.

If your network uses multiple LDAP/AD servers with referrals, then select one as the primary server (probably the one that holds the bulk of the users) and use the above settings for that server. It will then refer the SonicWALL on to the other servers for users in domains other than its own. For the SonicWALL to be able to log in to those other servers, each server must have a user configured with the same credentials (user name, password

and location in the directory) as the login to the primary server. This may entail creating a special user in the directory for the SonicWALL login. Note that only read access to the directory is required.

**Step 6** On the **Schema** tab, configure the following fields:

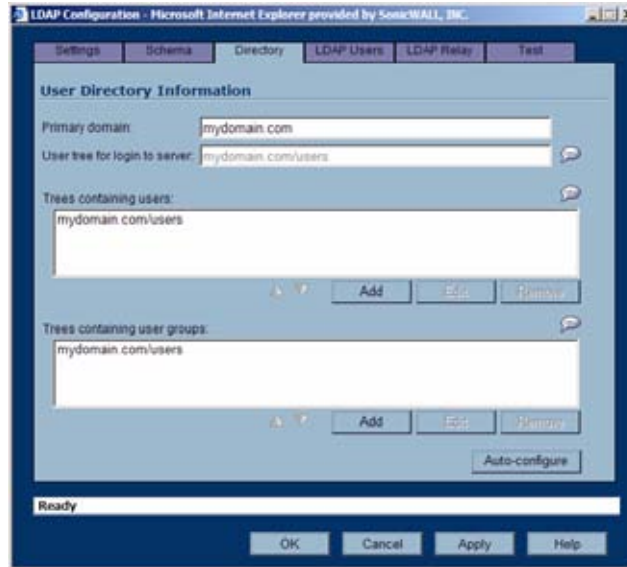


- **LDAP Schema** – Select one of the following:
  - Microsoft Active Directory
  - RFC2798 inetOrgPerson
  - RFC2307 Network Information Service
  - Samba SMB
  - Novell eDirectory
  - User defined

Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting **User defined** will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.
- **Object class** – Select the attribute that represents the individual user account to which the next two fields apply.
- **Login name attribute** – Select one of the following to define the attribute that is used for login authentication:
  - **sAMAccountName** for Microsoft Active Directory
  - **inetOrgPerson** for RFC2798 inetOrgPerson
  - **posixAccount** for RFC2307 Network Information Service
  - **sambaSAMAccount** for Samba SMB
  - **inetOrgPerson** for Novell eDirectory
- **Qualified login name attribute** – Optionally select an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.

- **User group membership attribute** – Select the attribute that contains information about the groups to which the user object belongs. This is **memberOf** in Microsoft Active Directory. The other pre-defined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- **Framed IP address attribute** – Select the attribute that can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting via L2TP with the SonicWALL's L2TP server. In the future this may also be supported for Global VPN Client. In Active Directory the static IP address is configured on the Dial-in tab of a user's properties.

**Step 7** On the **Directory** tab, configure the following fields:



- **Primary Domain** – The user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, e.g. *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.
- **User tree for login to server** – The tree in which the user specified in the **Settings** tab resides. For example, in Active Directory the 'administrator' account's default tree is the same as the user tree.
- **Trees containing users** – The trees where users commonly reside in the LDAP directory. One default value is provided which can be edited, and up to a total of 64 DN values may be provided. The SonicWALL will search the directory using them all until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- **Trees containing user groups** – Same as above, only with regard to user group containers, and a maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

All the above trees are normally given in URL format but can alternatively be specified as distinguished names (e.g. "myDom.com/Sales/Users" could alternatively be given as the DN "ou=Users,ou=Sales,dc=myDom,dc=com"). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



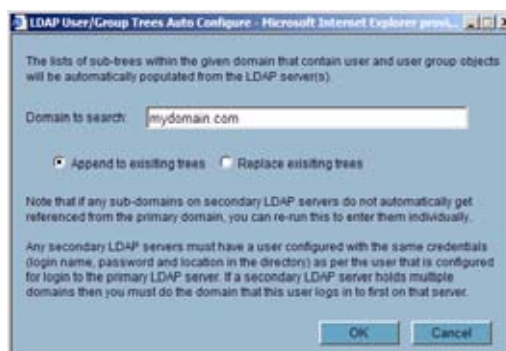
**Note** AD has some built-in containers that do not conform (e.g. the DN for the top level Users container is formatted as “cn=Users,dc=...”, using ‘cn’ rather than ‘ou’) but the SonicWALL knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.



**Note** When working with AD, to determine the location of a user in the directory for the ‘User tree for login to server’ field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- **Auto-configure** – This causes the SonicWALL to auto-configure the **Trees containing users** and **Trees containing user groups** fields by scanning through the directory/ directories looking for all trees that contain user objects. To use auto-configure, first enter a value in the **User tree for login to server** field (unless anonymous login is set), and then click the **Auto-configure** button to bring up the following dialog:



In the Auto Configure dialog box, enter the desired domain in the **Domain to search** field.

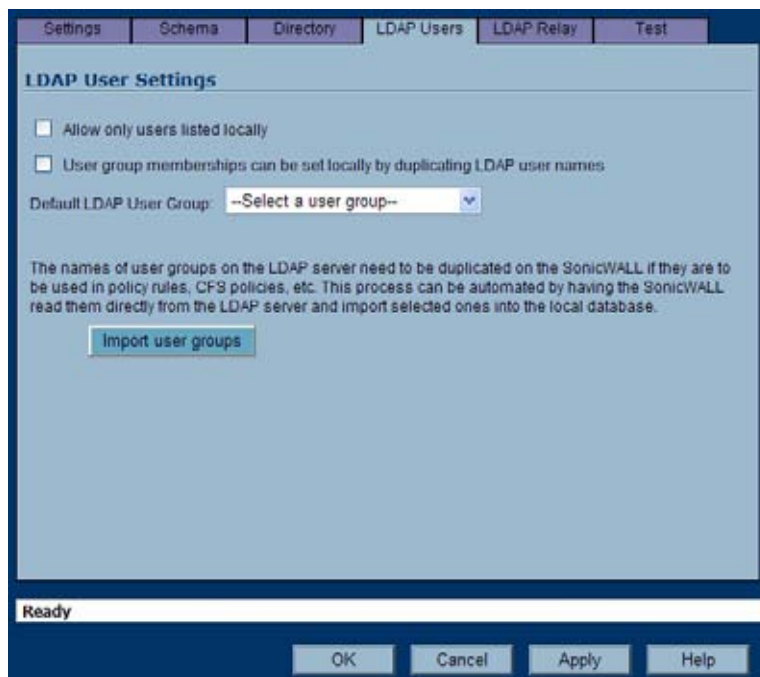
Select one of the following:

- **Append to existing trees** – This selection will append newly located trees to the current configuration.
- **Replace existing trees** – This selection will start from scratch removing all currently configured trees first.
- Click **OK**.

The auto-configuration process may also locate trees that are not needed for user login. You can manually remove these entries.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the **Domain to search** value accordingly and selecting **Append to existing trees** on each subsequent run.

**Step 8** On the **LDAP Users** tab, configure the following fields:



- **Allow only users listed locally** – Requires that LDAP users also be present in the SonicWALL local user database for logins to be allowed.
- **User group membership can be set locally by duplicating LDAP user names** – Allows for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- **Default LDAP User Group** – A default group on the SonicWALL to which LDAP users will belong in addition to group memberships configured on the LDAP server.

- **Import user groups** – You can click this button to configure user groups on the SonicWALL by retrieving the user group names from your LDAP server. The **Import user groups** button launches a dialog box containing the list of user group names available for import to the SonicWALL.



In the LDAP Import User Groups dialog box, select the checkbox for each group that you want to import into the SonicWALL, and then click Save.

Having user groups on the SonicWALL with the same name as existing LDAP/AD user groups allows SonicWALL group memberships and privileges to be granted upon successful LDAP authentication.

Alternatively, you can manually create user groups on the LDAP/AD server with the same names as SonicWALL built-in groups (such as 'Guest Services', 'Content Filtering Bypass', 'Limited Administrators') and assign users to these groups in the directory. This also allows SonicWALL group memberships to be granted upon successful LDAP authentication.

The SonicWALL appliance can retrieve group memberships efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

**Step 9** On the **LDAP Relay** tab, configure the following fields:



The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWALL with remote satellite sites connected into it via low-end SonicWALL security appliances that may not support LDAP. In that case the central SonicWALL can operate as a RADIUS server for the remote SonicWALLs, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWALLs running non-enhanced firmware, with this feature the central SonicWALL can return legacy user privilege information to them based on user group memberships learned via LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWALLs.

- **Enable RADIUS to LDAP Relay** – Enables this feature.
- **Allow RADIUS clients to connect via** – Check the relevant checkboxes and policy rules will be added to allow incoming RADIUS requests accordingly.
- **RADIUS shared secret** – This is a shared secret common to all remote SonicWALLs.
- **User groups for legacy VPN users** – Defines the user group that corresponds to the legacy 'Access to VPNs' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.
- **User groups for legacy VPN client users** – Defines the user group that corresponds to the legacy 'Access from VPN client with XAUTH' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.
- **User groups for legacy L2TP users** – Defines the user group that corresponds to the legacy 'Access from L2TP VPN client' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.
- **User groups for legacy users with Internet access** – Defines the user group that corresponds to the legacy 'Allow Internet access (when access is restricted)' privileges. When a user in this user group is authenticated, the remote SonicWALL is notified to give the user the relevant privileges.



**Note**

The 'Bypass filters' and 'Limited management capabilities' privileges are returned based on membership to user groups named 'Content Filtering Bypass' and 'Limited Administrators' – these are not configurable.

**Step 10** Select the **Test** tab to test the configured LDAP settings:

The **Test LDAP Settings** page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

## Configuring Single Sign-On

Configuring SSO is a process that includes installing and configuring the SonicWALL SSO Agent and configuring a SonicWALL security appliance running SonicOS Enhanced 4.0 to use the SSO Agent. This section contains the following subsections:

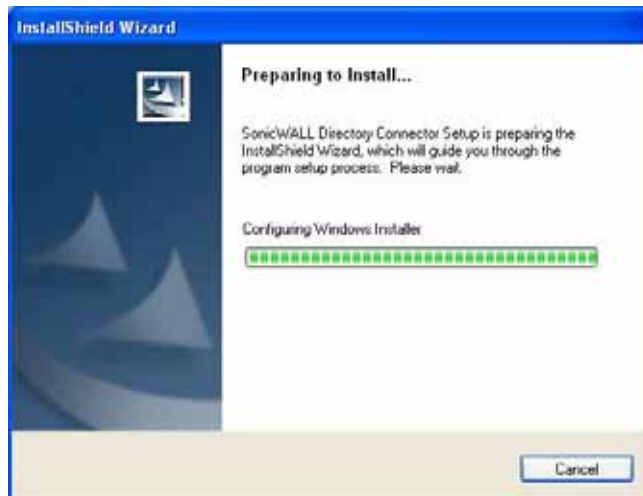
- [“Installing the SonicWALL SSO Agent” section on page 643](#)
- [“Configuring the SonicWALL SSO Agent” section on page 648](#)
  - [“Adding a SonicWALL Security Appliance” section on page 653](#)
  - [“Editing Appliances in SonicWALL SSO Agent” section on page 654](#)
  - [“Deleting Appliances in SonicWALL SSO Agent” section on page 654](#)
  - [“Modifying Services in SonicWALL SSO Agent” section on page 655](#)
- [“Configuring Your SonicWALL Security Appliance” section on page 655](#)
  - [“Advanced LDAP Configuration” section on page 661](#)
- [“Configuring Firewall Access Rules” section on page 669](#)
  - [“Viewing User Status” section on page 669](#)

- [“Configuring User Settings” section on page 669](#)

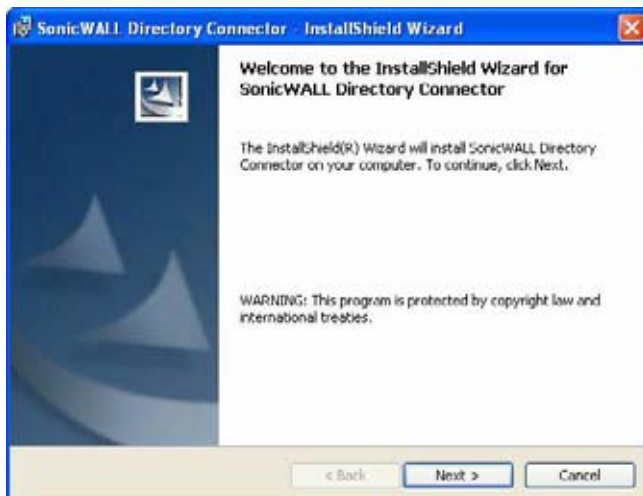
## Installing the SonicWALL SSO Agent

The SonicWALL SSO Agent is part of the SonicWALL Directory Connector. The SonicWALL SSO Agent must be installed on a workstation or server in the Windows domain that is accessible using VPN or IP. The SonicWALL SSO Agent must have access to your SonicWALL security appliance running SonicOS 4.0 or higher. To install the SonicWALL SSO Agent, perform the following steps:

- Step 1** Locate the SonicWALL Directory Connector executable file and double click it. It may take several seconds for the InstallShield to prepare for the installation.



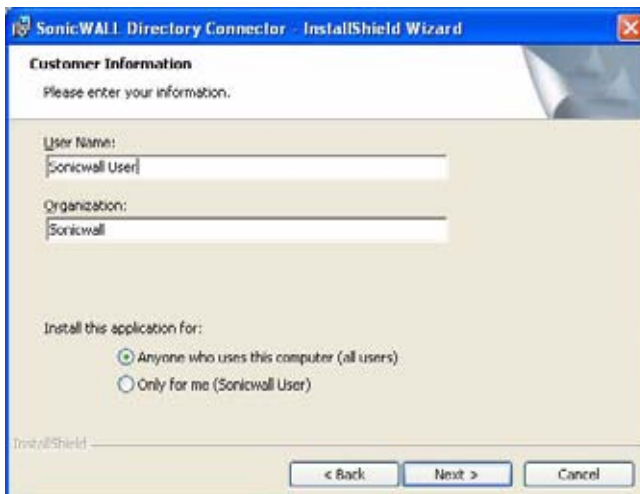
- Step 2** On the Welcome page, click **Next** to continue.



- Step 3** The License Agreement displays. Select **I accept the terms in the license agreement** and click **Next** to continue.




**Step 4** On the Customer Information page, enter your name in the **User Name** field and your organization name in the **Organization** field. Select to install the application for **Anyone who uses this computer (all users)** or **Only for me**. Click **Next** to continue.

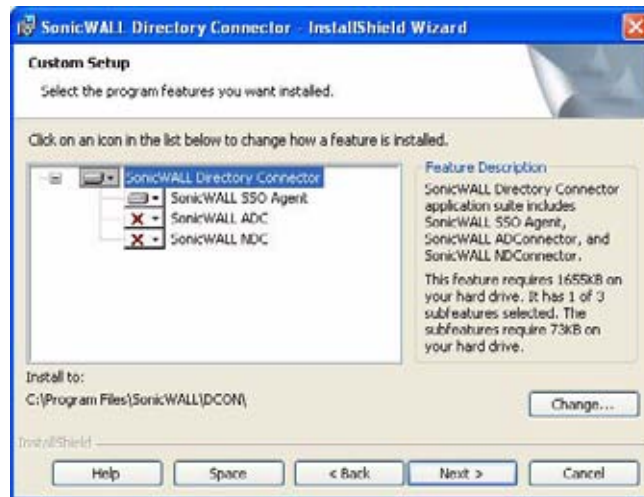


**Step 5** Select the destination folder. To use the default folder, C:\Program Files\SonicWALL\DCON, click **Next**. To specify a custom location, click **Browse**, select the folder, and click **Next**.

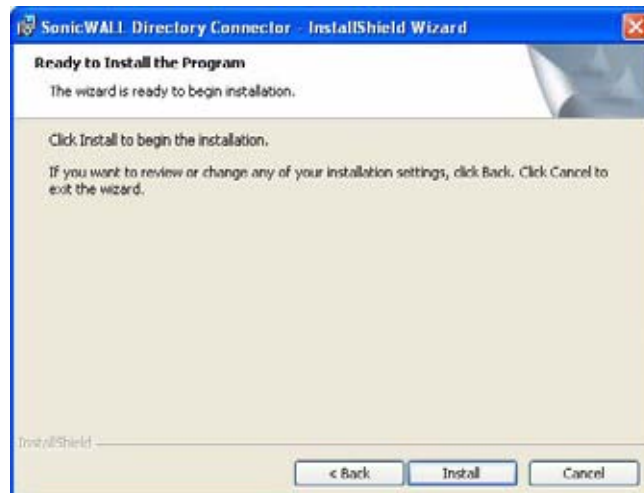


**Step 6** On the Custom Setup page, the installation icon  is displayed by default next to the

SonicWALL SSO Agent feature. Click **Next**.



**Step 7** Click **Install** to install SSO Agent.



**Step 8** To configure a common service account that the SSO Agent will use to log into a specified Windows domain, enter the username of an account with administrative privileges in the **Username** field, the password for the account in the **Password** field, and the domain name of the account in the **Domain Name** field. Click **Next**.

**Note**

This section can be configured at a later time. To skip this step and configure it later, click **Skip**.

- Step 9** Enter the IP address of your SonicWALL security appliance running SonicOS Enhanced 4.0 in the **SonicWALL Appliance IP** field. Type the port number for the same appliance in the **SonicWALL Appliance Port** field. Enter a shared key (a hexadecimal number from 1 to 16 digits in length) in the **Shared Key** field. Click **Next** to continue.

**Note**

This information can be configured at a later time. To skip this step and configure it later, leave the fields blank and click **Next**.

The SonicWALL SSO Agent installs. The status bar displays.



**Step 10** When installation is complete, optionally check the **Launch SonicWALL Directory Connector** box to launch the SonicWALL Directory Connector, and click **Finish**.



If you checked the **Launch SonicWALL Directory Connector** box, the SonicWALL Directory Connector will display.



## Configuring the SonicWALL SSO Agent

The SonicWALL SSO Agent communicates with workstations using NetAPI or WMI, which both provide information about users that are logged into a workstation, including domain users, local users, and Windows services. WMI is pre-installed on Windows Server 2003, Windows XP, Windows ME, and Windows 2000. For other Windows versions, visit [www.microsoft.com](http://www.microsoft.com) to download WMI. Verify that WMI or NetAPI is installed prior to configuring the SonicWALL SSO Agent.

The .NET Framework 2.0 must be installed prior to configuring the SonicWALL SSO Agent. The .NET Framework can be downloaded from Microsoft at [www.microsoft.com](http://www.microsoft.com).



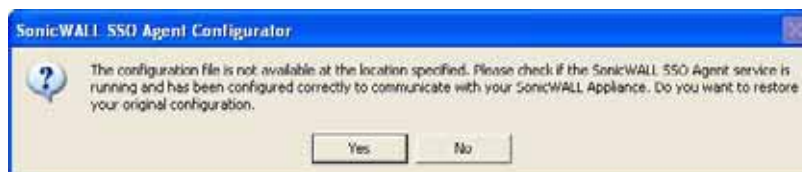
To configure the communication properties of the SonicWALL SSO Agent, perform the following tasks:

- Step 1** Launch the SonicWALL Configuration Tool by double-clicking the desktop shortcut or by navigating to **Start > All Programs > SonicWALL > SonicWALL Directory Connector > SonicWALL Configuration Tool**.

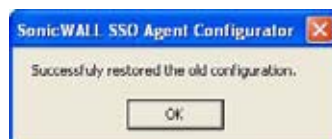


**Note**

If the IP address for a default SonicWALL security appliance was not configured, or if it was configured incorrectly, a pop up will display. Click **Yes** to use the default IP address (192.168.168.168) or click **No** to use the current configuration.




If you clicked **Yes**, the message **Successfully restored the old configuration** will display. Click **OK**.

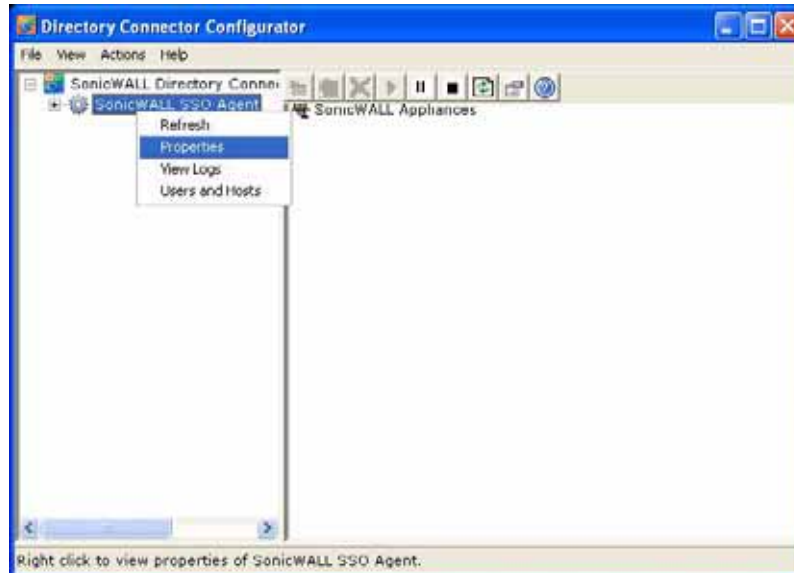


If you clicked **No**, or if you clicked **Yes** but the default configuration is incorrect, the message **SonicWALL SSO Agent service is not running. Please check the configuration and start the service.** will display. Click **OK**.



If the message **SonicWALL SSO Agent service is not running. Please check the configuration and start the service** displays, the SSO Agent service will be disabled by default. To enable the service, expand the SonicWALL Directory Connector Configuration Tool in the left navigation panel by clicking the + icon, highlight the SonicWALL SSO Agent underneath it, and click the  button.

- Step 2** In the left-hand navigation panel, expand the SonicWALL Directory Connector Configuration Tool by clicking the + icon. Right click the **SonicWALL SSO Agent** and select **Properties**.

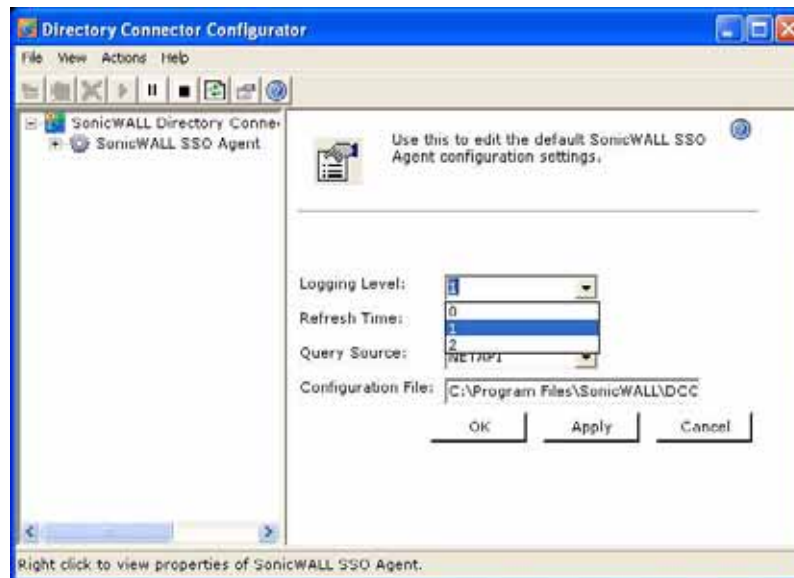


- Step 3** From the **Logging Level** pull-down menu, select the level of events to be logged in the Windows Event Log. The default logging level is 1. Select one of the following levels:

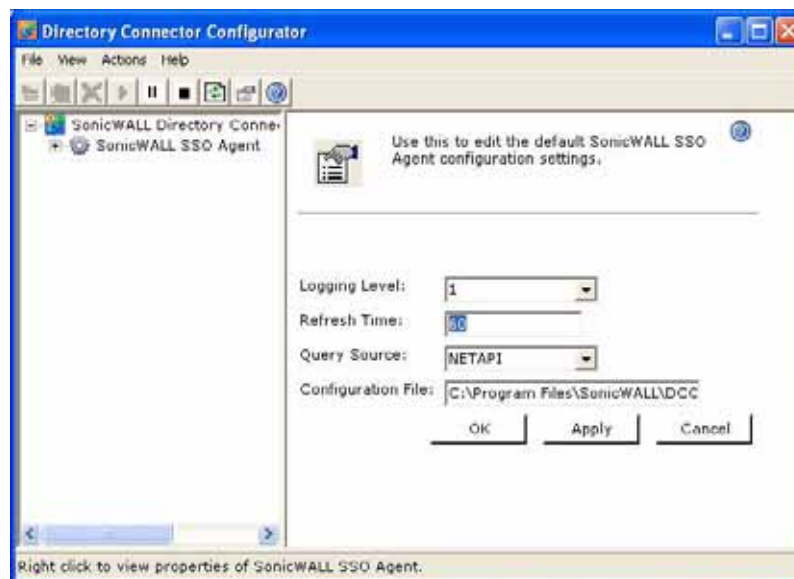
- **Logging Level 0** - Only critical events are logged.
- **Logging Level 1** - Critical and significantly severe events are logged.
- **Logging Level 2** - All requests from the appliance are logged, using the debug level of severity.

**Note**

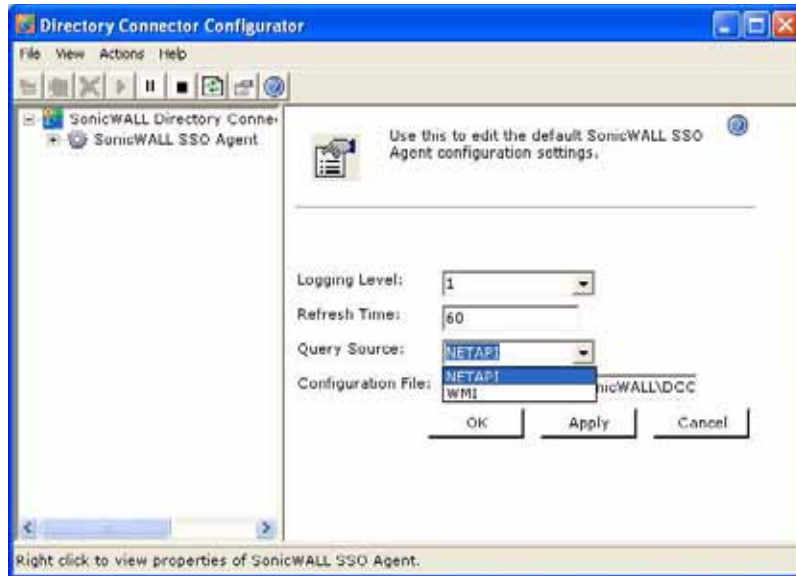
When Logging Level 2 is selected, the SSO Agent service will terminate if the Windows event log reaches its maximum capacity.



- Step 4** In the **Refresh Time** field, enter the frequency, in seconds, that the SSO Agent will refresh user log in status. The default is 60 seconds.

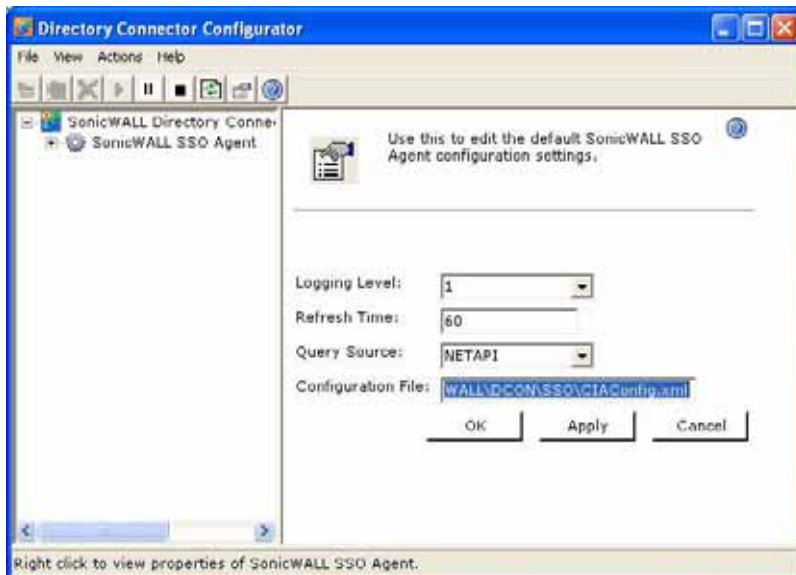


- Step 5** From the **Query Source** pull-down menu, select the protocol that the SSO Agent will use to communicate with workstations, either **NETAPI** or **WMI**.



**Note** NetAPI will provide faster, though possibly slightly less accurate, performance. WMI will provide slower, though possibly more accurate, performance. WMI is pre-installed on Windows Server 2003, Windows XP, Windows Me, and Windows 2000. Both NetAPI and WMI can be manually downloaded and installed. NetAPI and WMI provide information about users that are logged into a workstation, including domain users, local users, and Windows services.

**Step 6** In the **Configuration File** field, enter the path for the configuration file. The default path is **C:\Program Files\SonicWALL\DCC\SSO\CIAConfig.xml**.



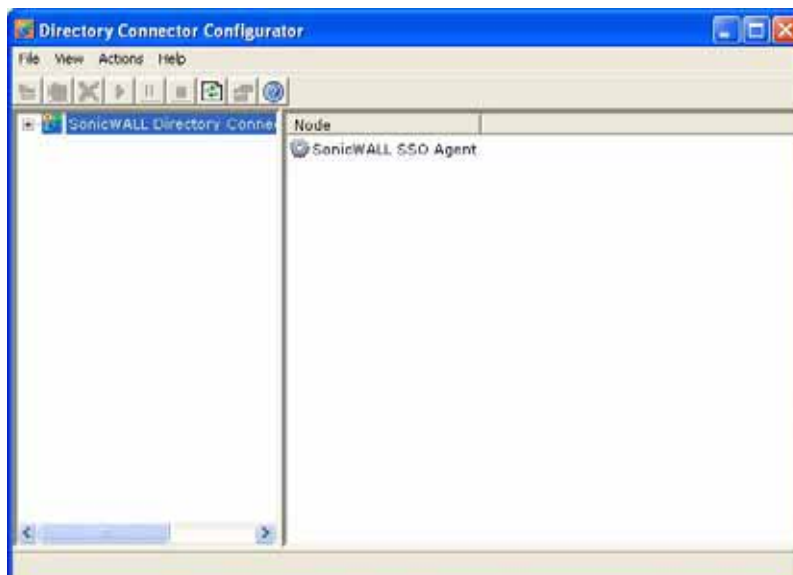
**Step 7** Click **Apply**.

**Step 8** Click **OK**.

## Adding a SonicWALL Security Appliance

Use these instructions to manually add a SonicWALL security appliance if you did not add one during installation, or to add additional SonicWALL security appliances. To add a SonicWALL security appliance, perform the following steps:

- Step 1** Launch the SonicWALL SSO Agent Configurator.



- Step 2** Expand the SonicWALL Directory Connector and SonicWALL SSO Agent trees in the left column by clicking the + button. Right click **SonicWALL Appliances** and select **Add**.




- Step 3** Enter the appliance IP address for your SonicWALL security appliance in the **Appliance IP** field. Enter the port for the same appliance in the **Appliance Port** field. The default port is 2258. Give your appliance a friendly name in the **Friendly Name** field. Enter a shared key in the **Shared Key** field or click **Generate Key** to generate a shared key. When you are finished, click **OK**.




Your appliance will display in the left-hand navigation panel under the **SonicWALL Appliances** tree.






### Editing Appliances in SonicWALL SSO Agent

You can edit all settings on SonicWALL security appliances previously added in SonicWALL SSO Agent, including IP address, port number, friendly name, and shared key. To edit a SonicWALL security appliance in SonicWALL SSO Agent, select the appliance from the left-hand navigation panel and click the edit icon  above the left-hand navigation panel. You can also click the **Edit** tab at the bottom of the right-hand window.

### Deleting Appliances in SonicWALL SSO Agent

To delete a SonicWALL security appliance you previously added in SonicWALL SSO Agent, select the appliance from the left-hand navigation panel and click the delete icon  above the left-hand navigation panel.

## Modifying Services in SonicWALL SSO Agent

You can start, stop, and pause SonicWALL SSO Agent services to SonicWALL security appliances. To pause services for an appliance, select the appliance from the left-hand navigation panel and click the pause button . To stop services for an appliance, select the appliance from the left-hand navigation panel and click the stop button . To resume services, click the start button .



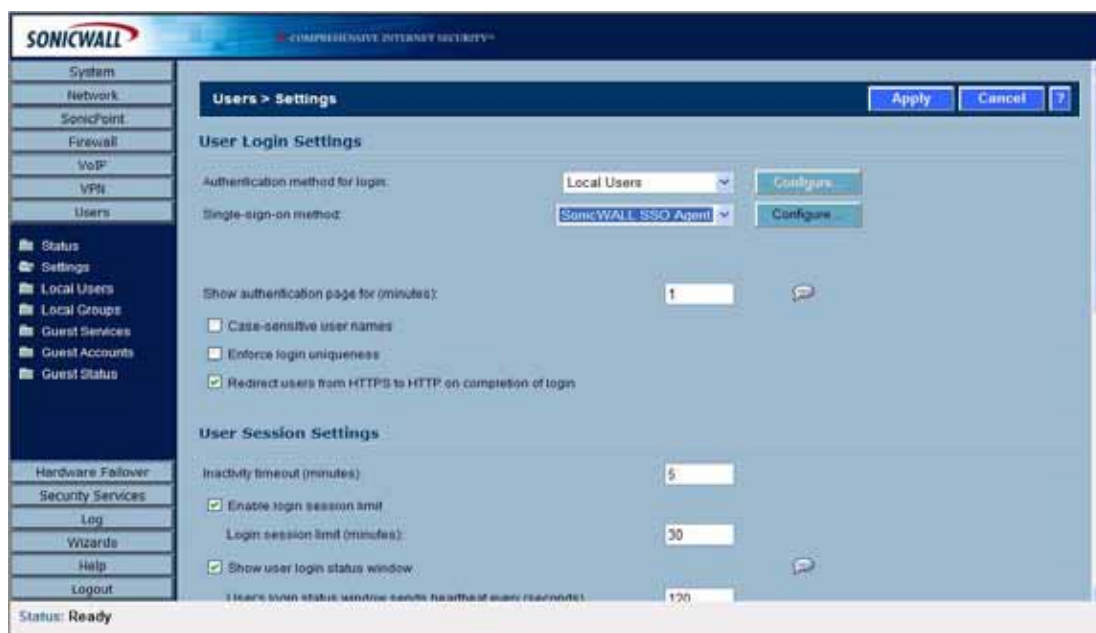
**Note** You may be prompted to restart services after making configuration changes to a SonicWALL security appliance in the SonicWALL SSO Agent. To restart services, press the stop button then press the start button.

## Configuring Your SonicWALL Security Appliance

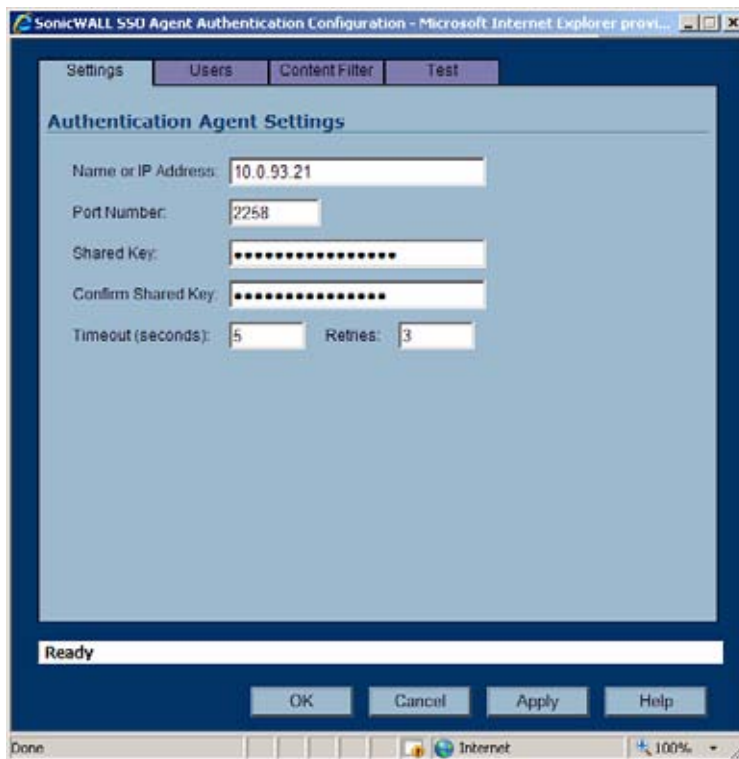
Your SonicWALL security appliance running SonicOS Enhanced 4.0 must be configured to use SonicWALL SSO Agent as the SSO method.

To configure your SonicWALL security appliance, perform the following steps:

- Step 1** Login to your SonicWALL security appliance running SonicOS Enhanced 4.0.
- Step 2** Navigate to **Users > Settings**.
- Step 3** In the **Single-sign-on method** drop-down menu, select **SonicWALL SSO Agent**.

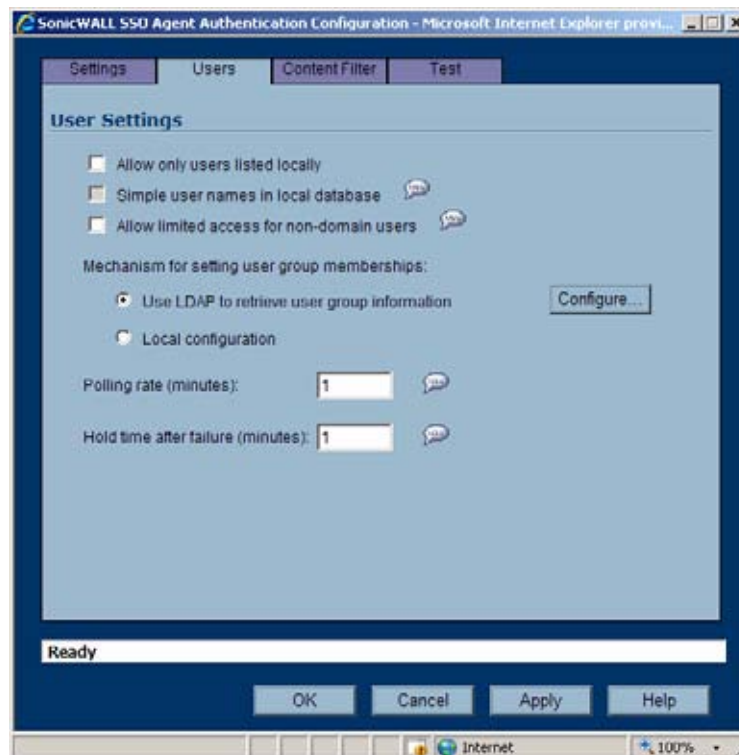


**Step 4** Click **Configure**. The Authentication Agent Settings page displays.



- Step 5** In the **Name or IP Address** field, enter the name or IP Address of the workstation on which SonicWALL SSO Agent is installed.
- Step 6** In **Port Number**, enter the port number of the workstation on which SonicWALL SSO Agent is installed. The default port is 2258.
- Step 7** In the **Shared Key** field, enter the shared key that you created or generated in the SonicWALL SSO Agent. The shared key must match exactly. Re-enter the shared key in the **Confirm Shared Key** field.
- Step 8** In the **Timeout (seconds)** field, enter a number of seconds before the authentication attempt times out.
- Step 9** In the **Retries** field, enter the number of authentication attempts.
- Step 10** Click the **Users** tab. The User Settings page displays.

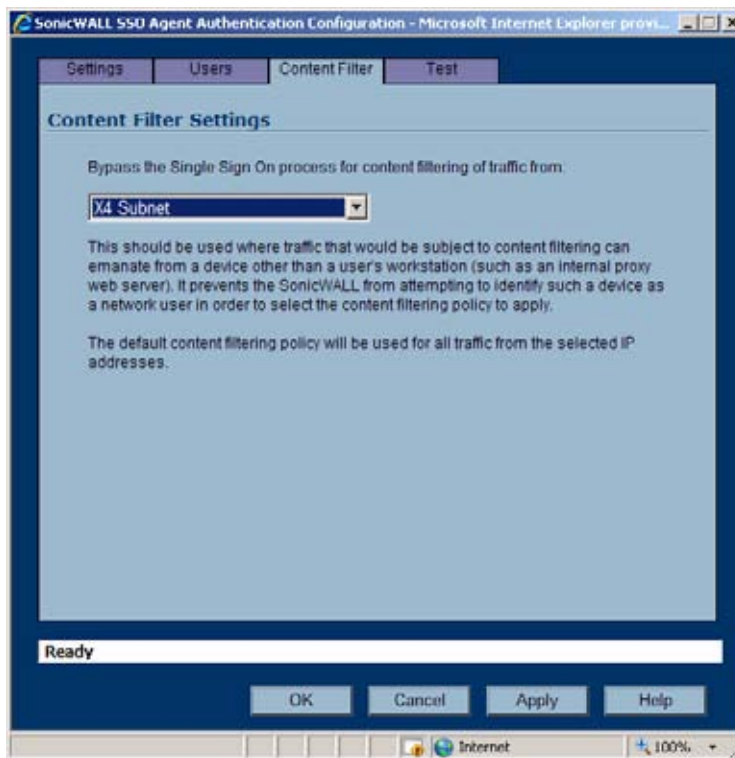




- Step 11** Check the box next to **Allow only users listed locally** to allow only users listed locally to be authenticated.
- Step 12** Check the box next to **Simple user names in local database** to use simple user names. This setting ignores the domain component of a user name. If this box is not checked, user names in the local database must match exactly the full names returned from the agent, including the domain component.
- Step 13** Check the box next to **Allow limited access for non-domain users** to allow limited access to users who are logged in to a computer but not into a domain. These users will not be given access to the Trusted Users user group. They are identified in logs as *computer-name/user-name*. When performing local authentication and the **Simple user names in local database** option is disabled, user names must be configured in the local database using the full *computer-name/user-name* identification.
- Step 14** To use LDAP to retrieve user information, select the **Use LDAP to retrieve user group information** radio button. Click **Configure** to configure the LDAP settings. The LDAP Configuration page displays. For configuration information for this page, refer to [“Advanced LDAP Configuration” section on page 661](#).
- Step 15** To use local configuration, select the **Local configuration** radio button.
- Step 16** In the **Polling rate (minutes)** field, enter a polling interval, in minutes, that the security appliance will poll the workstation running SSO Agent to verify that users are still logged on.
- Step 17** In the **Hold time after (minutes)** field, enter a time, in minutes, that the security appliance will wait before trying again to identify traffic after an initial failure to do so. This feature rate-limits requests to the agent.
- Step 18** Click on the **Content Filter** tab if you are using the SonicWALL Content Filtering Service (CFS) and there is a proxy server in your network.

**Note**

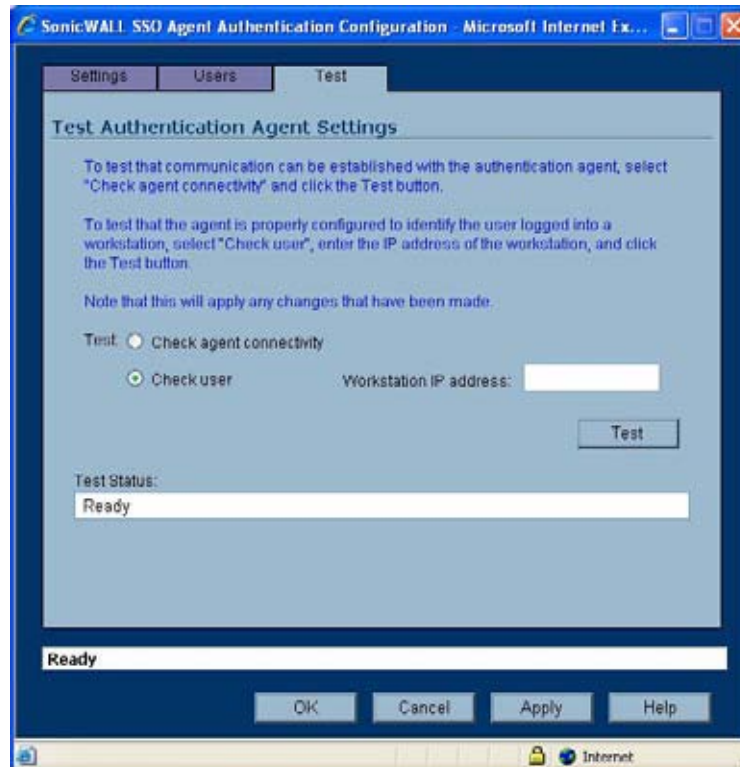
The **Content Filter** tab is only displayed if Premium CFS is enabled on the SonicWALL security appliance.



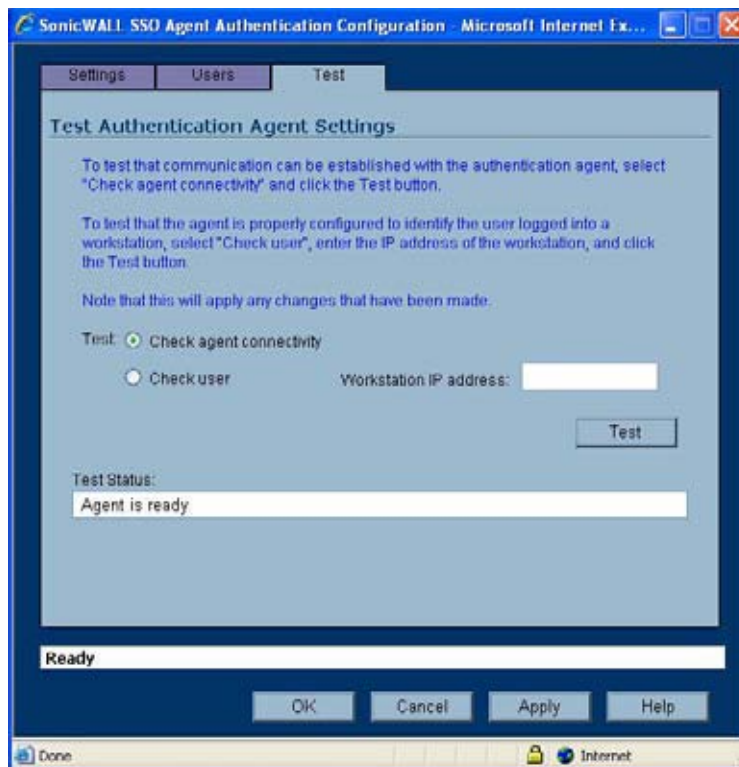
- Step 19** To bypass SSO for content filtering traffic and apply the default content filtering policy to the traffic, select the appropriate address object or address group from the pulldown menu.

This setting should be used where traffic that would be subject to content filtering can emanate from a device other than a user's workstation (such as an internal proxy web server). It prevents the SonicWALL from attempting to identify such a device as a network user in order to select the content filtering policy to apply. The default content filtering policy will be used for all traffic from the selected IP addresses.

**Step 20** Click the **Test** tab. The Test Authentication Agent Settings page displays.



**Step 21** Select the **Check agent connectivity** radio button then click the **Test** button. This will test communication with the authentication agent. If the SonicWALL security appliance can connect to the agent, you will see the message **Agent is ready**.



**Step 22** Select the **Check user** radio button, enter the IP address of a workstation in the **Workstation IP address** field, then click **Test**. This will test if the agent is properly configured to identify the user logged into a workstation.

**Note**


---

Performing tests on this page applies any changes that have been made.

---

**Tip**


---

If you receive the messages **Agent is not responding** or **Configuration error**, check your settings and perform these tests again.

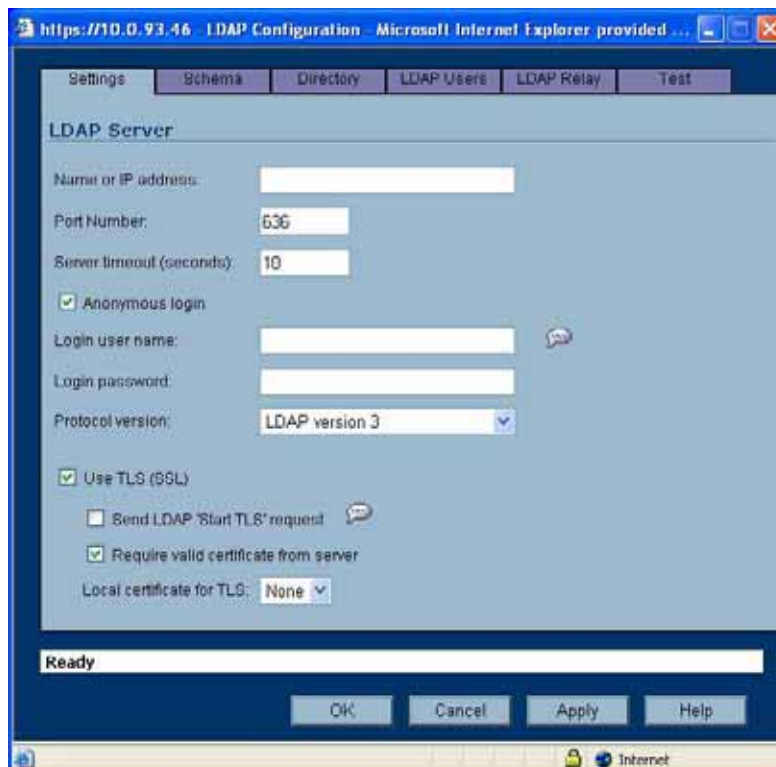
---

**Step 23** When you are finished, click **OK**.

## Advanced LDAP Configuration

If you selected **Use LDAP to retrieve user group information** in step 14 of “[Configuring Your SonicWALL Security Appliance](#)” section on page 655, you must configure your LDAP settings. To configure LDAP settings, perform the following steps:

- Step 1** The **Settings** tab displays. In the **Name or IP address** field, enter the name or IP address of your LDAP server.



- Step 2** In the **Port Number** field, enter the port number of your LDAP server. The default port is 636.
- Step 3** In the **Server timeout (seconds)** field, enter a number of seconds the SonicWALL security appliance will wait for a response from the LDAP server before the attempt times out. Allowable values are 1 to 99999. The default is 10 seconds.
- Step 4** Check the **Anonymous login** box to login anonymously. Some LDAP servers allow for the tree to be accessed anonymously. If your server supports this (MS AD generally does not), you may select this option.
- Step 5** To login with a user's name and password, enter the user's name in the **Login user name** field and the password in the **Login password** field. The login name will automatically be presented to the LDAP server in full 'dn' notation.



**Note**

Use the user's name in the **Login user name** field, not a username or login ID. For example, John Doe would login as John Doe, not jdoe.

- Step 6** Select the LDAP version from the **Protocol version** drop-down menu, either LDAP version 2 1 (LDAPv2) or LDAP version 3 (LDAPv3). Most implementations of LDAP, including AD, employ LDAPv3.
- Step 7** Check the **Use TLS (SSL)** box to use Transport Layer Security (SSL) to login to the LDAP server. It is strongly recommended to use TLS to protect the username and password information that will be sent across the network. Most implementations of LDAP server, including AD, support TLS.
- Step 8** Check the **Send LDAP 'Start TLS' request** to allow the LDAP server to operate in TLS and non-TLS mode on the same TCP port. Some LDAP server implementations support the Start TLS directive rather than using native LDAP over TLS. This allows the LDAP server to listen on one port (normally 389) for LDAP connections, and to switch to TLS as directed by the client. AD does not use this option, and it should only be selected if required by your LDAP server.



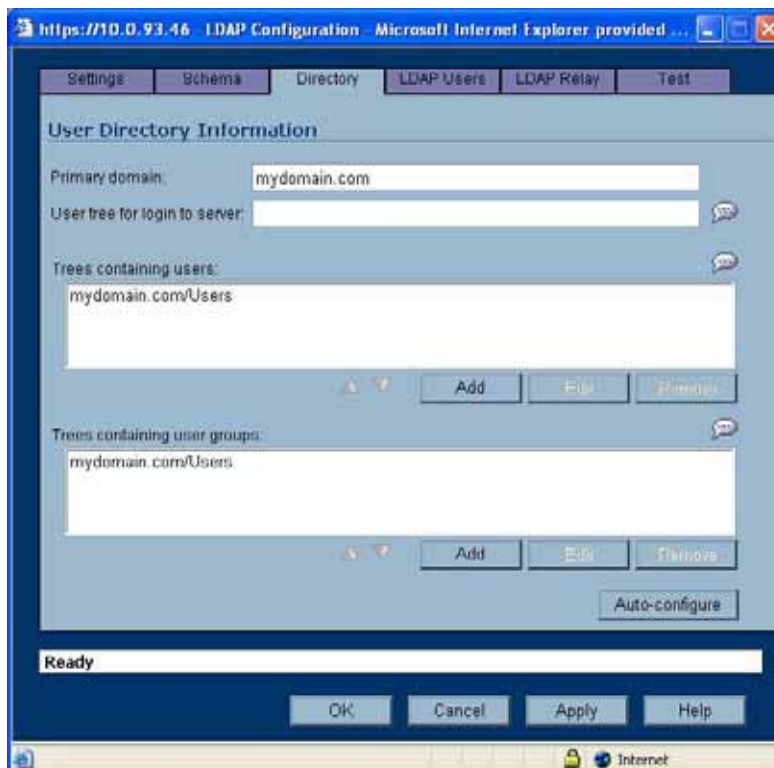
**Note** Only check the **Send LDAP 'Start TLS' request** box if your LDAP server uses the same port number for TLS and non-TLS.

- Step 9** Check the **Require valid certificate from server** to require a valid certificate from the server. Validates the certificate presented by the server during the TLS exchange, matching the name specified above to the name on the certificate. Deselecting this default option will present an alert, but exchanges between the SonicWALL security appliance and the LDAP server will still use TLS – only without issuance validation.
- Step 10** Select a local certificate from the **Local certificate for TLS** drop-down menu. This is optional, to be used only if the LDAP server requires a client certificate for connections. This feature is useful for LDAP server implementations that return passwords to ensure the identity of the LDAP client (AD does not return passwords). This setting is not required for AD.
- Step 11** Click **Apply**.
- Step 12** Click the **Schema** tab.

**Step 13** From the **LDAP Schema** pull-down menu, select one of the following LDAP schemas. Selecting any of the predefined schemas will automatically populate the fields used by that schema with their correct values. Selecting 'user-defined' will allow you to specify your own values – use this only if you have a specific or proprietary LDAP schema configuration.

- Microsoft Active Directory
- RFC2798 InetOrgPerson
- RFC2307 Network Information Service
- Samba SMB
- Novell eDirectory
- User defined

- Step 14** The **Object class** field defines which attribute represents the individual user account to which the next two fields apply. This will not be modifiable unless you select **User defined**.
- Step 15** The **Login name attribute** field defines which attribute is used for login authentication. This will not be modifiable unless you select **User defined**.
- Step 16** If the **Qualified login name attribute** field is not empty, it specifies an attribute of a user object that sets an alternative login name for the user in *name@domain* format. This may be needed with multiple domains in particular, where the simple login name may not be unique across domains. This is set to **mail** for Microsoft Active Directory and RFC2798 inetOrgPerson.
- Step 17** The **User group membership attribute** field contains the information in the user object of which groups it belongs to. This is **memberOf** in Microsoft Active Directory. The other pre-defined schemas store group membership information in the group object rather than the user object, and therefore do not use this field.
- Step 18** The **Framed IP address attribute** field can be used to retrieve a static IP address that is assigned to a user in the directory. Currently it is only used for a user connecting using L2TP with the SonicWALL security appliance L2TP server. In future releases, this may also be supported for the SonicWALL Global VPN Client (GVC). In Active Director, the static IP address is configured on the Dial-in tab of a user's properties.
- Step 19** The **Object class** field defines the type of entries that an LDAP directory may contain. A sample object class, as used by AD, would be 'user' or 'group'.
- Step 20** The **Member attribute** field defines which attribute is used for login authentication.
- Step 21** Select the **Directory** tab.



- Step 22** In the **Primary Domain** field, specify the user domain used by your LDAP implementation. For AD, this will be the Active Directory domain name, such as *yourADdomain.com*. Changes to this field will, optionally, automatically update the tree information in the rest of the page. This is set to **mydomain.com** by default for all schemas except Novell eDirectory, for which it is set to **o=mydomain**.



- Step 23** In the **User tree for login to server** field, specify the tree in which the user specified in the 'Settings' tab resides. For example, in AD the 'administrator' account's default tree is the same as the user tree.
- Step 24** In the **Trees containing users** field, specify the trees where users commonly reside in the LDAP directory. One default value is provided that can be edited, a maximum of 64 DN values may be provided, and the SonicWALL security appliance searches the directory until a match is found, or the list is exhausted. If you have created other user containers within your LDAP or AD directory, you should specify them here.
- Step 25** In the **Trees containing user groups** specify the trees where user groups commonly reside in the LDAP directory. A maximum of 32 DN values may be provided. These are only applicable when there is no user group membership attribute in the schema's user object, and are not used with AD.

The above-mentioned trees are normally given in URL format but can alternatively be specified as distinguished names (for example, "myDom.com/Sales/Users" could alternatively be given as the DN "ou=Users,ou=Sales,dc=myDom,dc=com"). The latter form will be necessary if the DN does not conform to the normal formatting rules as per that example. In Active Directory the URL corresponding to the distinguished name for a tree is displayed on the Object tab in the properties of the container at the top of the tree.



**Note** AD has some built-in containers that do not conform (for example, the DN for the top level Users container is formatted as "cn=Users,dc=...", using 'cn' rather than 'ou') but the SonicWALL knows about and deals with these, so they can be entered in the simpler URL format.

Ordering is not critical, but since they are searched in the given order it is most efficient to place the most commonly used trees first in each list. If referrals between multiple LDAP servers are to be used, then the trees are best ordered with those on the primary server first, and the rest in the same order that they will be referred.



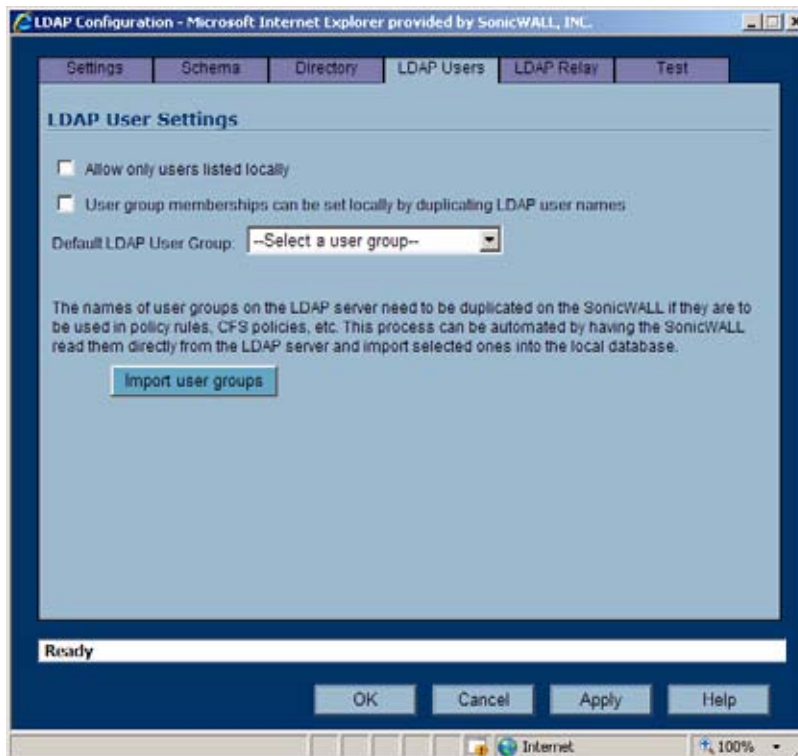
**Note** When working with AD, to locate the location of a user in the directory for the 'User tree for login to server' field, the directory can be searched manually from the Active Directory Users and Settings control panel applet on the server, or a directory search utility such as queryad.vbs in the Windows NT/2000/XP Resource Kit can be run from any PC in the domain.

- Step 26** The **Auto-configure** button causes the SonicWALL security appliance to auto-configure the 'Trees containing users' and 'Trees containing user groups' fields by scanning through the directory/directories looking for all trees that contain user objects. The 'User tree for login to server' must first be set.

Select whether to append new located trees to the current configuration, or to start from scratch removing all currently configured trees first, and then click **OK**. Note that it will quite likely locate trees that are not needed for user login and manually removing such entries is recommended.

If using multiple LDAP/AD servers with referrals, this process can be repeated for each, replacing the 'Domain to search' accordingly and selecting 'Append to existing trees' on each subsequent run.

**Step 27** Select the **LDAP Users** tab.



- Step 28** Check the **Allow only users listed locally** box to require that LDAP users also be present in the SonicWALL security appliance local user database for logins to be allowed.
- Step 29** Check the **User group membership can be set locally by duplicating LDAP user names** box to allow for group membership (and privileges) to be determined by the intersection of local user and LDAP user configurations.
- Step 30** From the **Default LDAP User Group** pull-down menu, select a default group on the SonicWALL security appliance to which LDAP users will belong in addition to group memberships configured on the LDAP server.

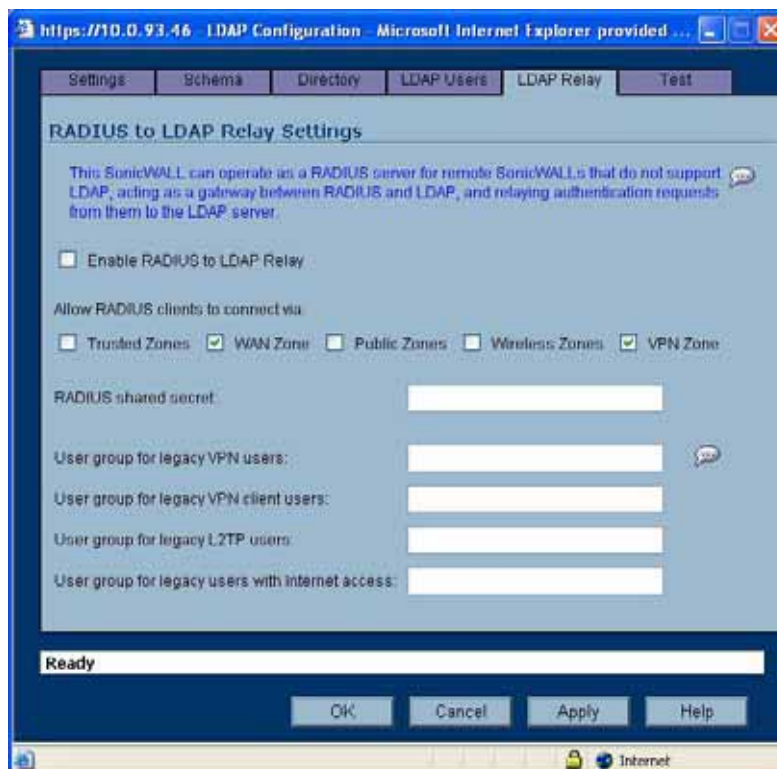


**Tip**

Group memberships (and privileges) can also be assigned simply with LDAP. By creating user groups on the LDAP/AD server with the same name as SonicWALL security appliance built-in groups (such as **Guest Services**, **Content Filtering Bypass**, **Limited Administrators**) and assigning users to these groups in the directory, or creating user groups on the SonicWALL security appliance with the same name as existing LDAP/AD user groups, SonicWALL group memberships will be granted upon successful LDAP authentication.

The SonicWALL security appliance can retrieve group memberships more efficiently in the case of Active Directory by taking advantage of its unique trait of returning a 'memberOf' attribute for a user.

- Step 31** Click the **Import user groups** button to import user groups from the LDAP server. The names of user groups on the LDAP server need to be duplicated on the SonicWALL if they are to be used in policy rules, CFS policies, etc.
- Step 32** Select the **LDAP Relay** tab.



- Step 33** Check the **Enable RADIUS to LDAP Relay** box to enable RADIUS to LDAP relay. The RADIUS to LDAP Relay feature is designed for use in a topology where there is a central site with an LDAP/AD server and a central SonicWALL security appliance with remote satellite sites connected into it using SonicWALL security appliances that may not support LDAP. In that case the central SonicWALL security appliance can operate as a RADIUS server for the remote SonicWALL security appliances, acting as a gateway between RADIUS and LDAP, and relaying authentication requests from them to the LDAP server.

Additionally, for remote SonicWALL security appliances running non-enhanced firmware, with this feature the central SonicWALL security appliance can return legacy user privilege information to them based on user group memberships learned using LDAP. This avoids what can be very complex configuration of an external RADIUS server such as IAS for those SonicWALL security appliances.

- Step 34** Under **Allow RADIUS clients to connect via**, check the relevant checkboxes and policy rules will be added to allow incoming Radius requests accordingly. The options are:
- Trusted Zones
  - WAN Zone
  - Public Zones
  - Wireless Zones

– VPN Zone

- Step 35** In the **RADIUS shared secret** field, enter a shared secret common to all remote SonicWALL security appliances.
- Step 36** In the **User groups for legacy users** fields, define the user groups that correspond to the legacy ‘VPN users,’ ‘VPN client users,’ ‘L2TP users’ and ‘users with Internet access’ privileges. When a user in one of the given user groups is authenticated, the remote SonicWALL security appliances will be informed that the user is to be given the relevant privilege.



**Note** The ‘Bypass filters’ and ‘Limited management capabilities’ privileges are returned based on membership to user groups named ‘Content Filtering Bypass’ and ‘Limited Administrators’ – these are not configurable.

- Step 37** Select the **Test** tab.

The ‘Test’ page allows for the configured LDAP settings to be tested by attempting authentication with specified user and password credentials. Any user group memberships and/or framed IP address configured on the LDAP/AD server for the user will be displayed.

- Step 38** In the **Username** and **Password** fields, enter a valid LDAP login name for the LDAP server you configured.
- Step 39** Select **Password authentication** or **CHAP** (Challenge Handshake Authentication Protocol).



**Note** CHAP only works with a server that supports retrieving user passwords using LDAP and in some cases requires that the LDAP server to be configured to store passwords reversibly. CHAP cannot be used with Active Directory.

- Step 40** Click **Test**.

## Configuring Firewall Access Rules

Firewall access rules provide the administrator with the ability to control user access. Rules set under **Firewall > Access Rules** are checked against the user group memberships returned from a SSO LDAP query, and are applied automatically. Access rules are network management tools that allow you to define inbound and outbound access policy, configure user authentication, and enable remote management of the SonicWALL security appliance. The SonicOS **Firewall > Access Rules** page provides a sortable access rule management interface. The subsequent sections provide high-level overviews on configuring access rules by zones and configuring bandwidth management using access rules.



**Note** More specific policy rules should be given higher priority than general policy rules. The general specificity hierarchy is source, destination, service. User identification elements, for example, user name and corresponding group permissions, are not included in defining the specificity of a policy rule.

By default, SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet, and blocks all traffic to the LAN from the Internet.

Additional network access rules can be defined to extend or override the default access rules. For example, access rules can be created that block certain types of traffic such as IRC from the LAN to the WAN, or allow certain types of traffic, such as Lotus Notes database synchronization, from specific hosts on the Internet to specific hosts on the LAN, or restrict use of certain protocols such as Telnet to authorized users on the LAN.



**Note** The ability to define network access rules is a powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.

For detailed information about the **Firewall > Access Rules** page, refer to the *SonicOS Enhanced 4.0 Administrator's Guide*.

## Viewing User Status

The **Users > Status** page displays **Active User Sessions** on the SonicWALL security appliance. The table lists **User Name**, **IP Address**, **Session Time**, **Time Remaining**, **Inactivity Remaining**, **Settings**, and **Logout**. For users authenticated using SonicWALL SSO Agent, the message **Auth. by SSO Agent** will display. To logout a user, click the trash can icon next to the user's entry.



**Note** Changes in a user's settings, configured under **Users > Settings**, will not be reflected during that user's current session; you must manually log the user out for changes to take effect. The user will be transparently logged in again, with the changes reflected.

## Configuring User Settings

The **Users > Settings** page provides the administrator with configuration options for user session settings, global user settings, and acceptable use policy settings, in addition to SSO and other user login settings.

The **Enable login session limit** and corresponding **Login session limit (minutes)** settings under User Session Settings apply to users logged in using SSO. SSO users will be logged out according to session limit settings, but will be automatically and transparently logged back in when they send further traffic.



**Note**

Do not set the login session limit interval too low. This could potentially cause performance problems, especially for deployments with many users.

Changes applied in the **Users > Settings** page during an active SSO session will not be reflected during that session.



**Tip**

You must log the user out for changes to take effect. The user will immediately and automatically be logged in again, with the changes made.

## Configuring Multiple Administrator Support

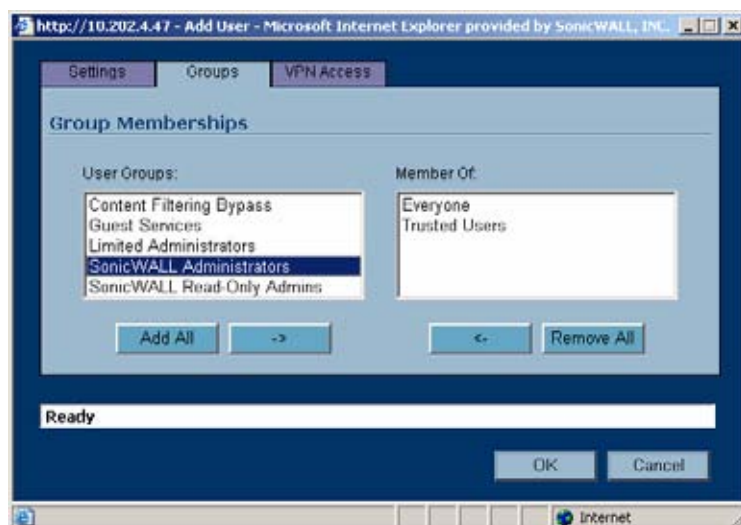
This section contains the following subsections:

- [“Configuring Additional Administrator User Profiles”](#) section on page 671
- [“Configuring Administrators Locally when Using LDAP or RADIUS”](#) section on page 671
- [“Preempting Administrators”](#) section on page 672
- [“Activating Configuration Mode”](#) section on page 673
- [“Verifying Multiple Administrators Support Configuration”](#) section on page 675
- [“Viewing Multiple Administrator Related Log Messages”](#) section on page 676

## Configuring Additional Administrator User Profiles

To configure additional administrator user profiles, perform the following steps:

- Step 1** While logged in as **admin**, navigate to the **Users > Local Users** page.
- Step 2** Click the **Add User** button.
- Step 3** Enter a **Name** and **Password** for the user.
- Step 4** Click on the **Group Membership** tab.



- Step 5** Select the appropriate group to give the user Administrator privileges:
  - Limited Administrators - The user has limited administrator configuration privileges.
  - SonicWALL Administrators - The user has full administrator configuration privileges.
  - SonicWALL Read-Only Admins - The user can view the entire management interface, but cannot make any changes to the configuration.
- Step 6** Click the right arrow button and click **OK**.
- Step 7** To configure the multiple administrator feature such that administrators are logged out when they are preempted, navigate to the **System > Administration** page.
- Step 8** Select the **Log out** radio button for the **On preemption by another administrator** option and click **Apply**.

## Configuring Administrators Locally when Using LDAP or RADIUS

When using RADIUS or LDAP authentication, if you want to ensure that some or all administrative users will always be able to manage the appliance, even if the RADIUS or LDAP server becomes unreachable, then you can use the **RADIUS + Local Users** or **LDAP + Local Users** option and configure the accounts for those particular users locally.

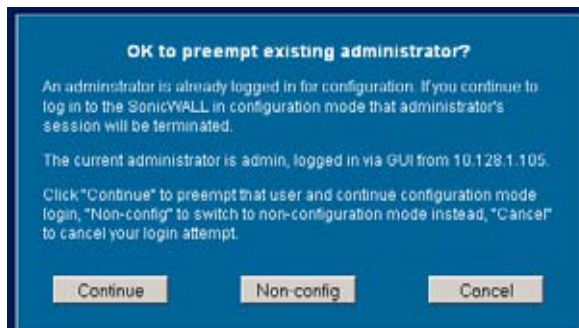
For users authenticated by RADIUS or LDAP, create user groups named **SonicWALL Administrators** and/or **SonicWALL Read-Only Admins** on the RADIUS or LDAP server (or its back-end) and assign the relevant users to those groups. Note that in the case of RADIUS you will probably need special configuration of the RADIUS server to return the user group information – see the SonicWALL RADIUS documentation for details.

When using RADIUS or LDAP authentication, if you want to keep the configuration of administrative users local to the appliance whilst having those users authenticated by RADIUS/ LDAP, perform these steps:

- Step 1** Navigate to the **Users > Settings** page.
- Step 2** Select either the **RADIUS + Local Users** or **LDAP + Local Users** authentication method.
- Step 3** Click the **Configure** button.
- Step 4** For RADIUS, click on the **RADIUS Users** tab and select the **Local configuration only radio** button and ensure that the **Memberships can be set locally by duplicating RADIUS user names** checkbox is checked.
- Step 5** For LDAP, click on the **LDAP Users** tab and select the **User group membership can be set locally by duplicating LDAP user names** checkbox.
- Step 6** Then create local user accounts with the user names of the administrative users (note no passwords need be set here) and add them to the relevant administrator user groups.

## Preempting Administrators

When an administrator attempts to log in while another administrator is logged in, the following message is displayed. The message displays the current administrator's user name, IP address, phone number (if it can be retrieved from LDAP), and whether the administrator is logged in using the GUI or CLI.



This window gives you three options:

- **Continue** - Preempts the current administrator. The current administrator is dropped to non-config mode and you are given full administrator access.
- **Non-config** - You are logged into the appliance in non-config mode. The current administrator's session is not disturbed.
- **Cancel** - Returns to the authentication screen.

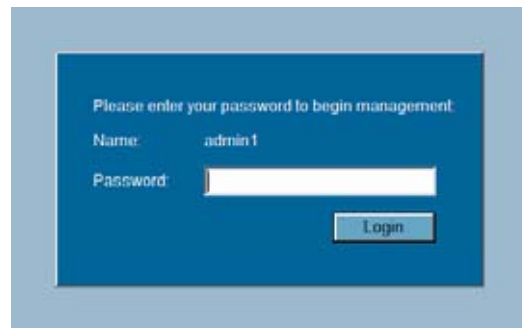


## Activating Configuration Mode

When logging in as a user with full administrator rights (that is not the **admin** user), the **User Login Status** window is displayed.



To go to the SonicWALL user interface, click the **Manage** button. You will be prompted to enter your password again. This is a safeguard to protect against unauthorized access when administrators are away from their computers and do not logout of their session.

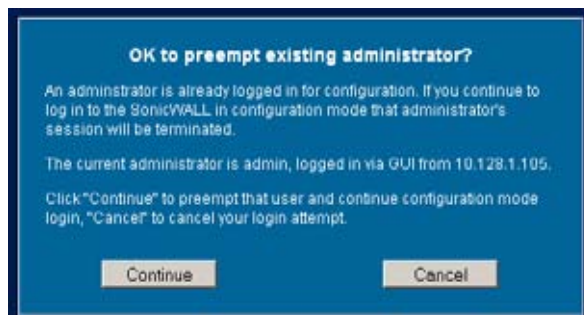


To switch from non-config mode to full configuration mode, perform the following steps:

**Step 1** Navigate to the **System > Administration** page.

**Step 2** In the **Web Management Settings** section, click on the **Configuration mode** button. If there is not currently an administrator in configuration mode, you will automatically be entered into configuration mode.

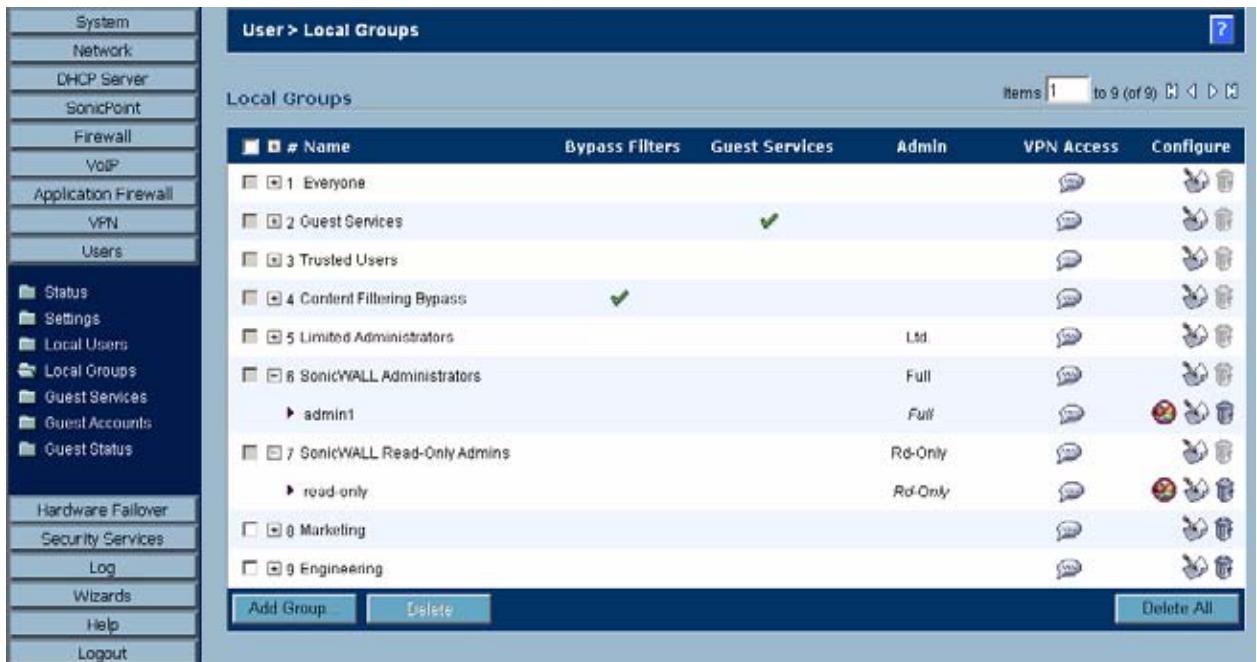
**Step 3** If another administrator is in configuration mode, the following message displays.



**Step 4** Click the **Continue** button to enter configuration mode. The current administrator is converted to read-only mode and you are given full administrator access.

## Verifying Multiple Administrators Support Configuration

User accounts with administrator and read-only administrators can be viewed on the **Users > Local Groups** page.



Administrators can determine which configuration mode they are in by looking at either the top right corner of the management interface or at the status bar of their browser.

To display the status bar in Firefox and Internet Explorer, click on the **View** menu and enable **status bar**. By default, Internet Explorer 7.0 and Firefox 2.0 do not allow webpages to display text in the status bar. To allow status bar messages in Internet Explorer, go to **Tools > Internet Options**, select the **Security** tab, click on the **Custom Level** button, scroll to the bottom of the list, and select **Enable** for **Allow Status Bar Updates Via Script**.

To allow status bar messages in Firefox, go to **Tools > Options**, select the **Content** tab, click the **Advanced** button, and select the checkbox for **Change Status Bar Text** in the pop-up window that displays.

When the administrator is in full configuration mode, no message is displayed in the top right corner and the status bar displays **Done**.



When the administrator is in read-only mode, the top right corner of the interface displays **Read-Only Mode**.



The status bar displays **Read-only mode - no changes can be made**.



When the administrator is in non-config mode, the top right of the interface displays **Non-Config Mode**. Clicking on this text links to the **System > Administration** page where you can enter full configuration mode.



The status bar displays **Non-config mode - configuration changes not allowed**.



## Viewing Multiple Administrator Related Log Messages

Log messages are generated for the following events:

- A GUI or CLI user begins configuration mode (including when an admin logs in).
- A GUI or CLI user ends configuration mode (including when an admin logs out).
- A GUI user begins management in non-config mode (including when an admin logs in and when a user in configuration mode is preempted and dropped back to read-only mode).
- A GUI user begins management in read-only mode.

A GUI user terminates either of the above management sessions (including when an admin logs out).

## CHAPTER 53

# Managing Guest Services and Guest Accounts

## Users > Guest Services

Guest accounts are temporary accounts set up for users to log into your network. You can create these accounts manually, as needed or generate them in batches. SonicOS includes profiles you can configure in advance to automate configuring guest accounts when you generate them. Guest accounts are typically limited to a pre-determined life-span. After their life span, by default, the accounts are removed.

Guest Services determine the limits and configuration of the guest accounts. The **Users > Guest Services** page displays a list of Guest Profiles. Guest profiles determine the configuration of guest accounts when they are generated. In the **Users > Guest Services** page, you can add, delete, and configure Guest Profiles. In addition, you can determine if all users who log in to the security appliance see a user login window that displays the amount of time remaining in their current login session.



Name	User Name Prefix	Account Lifetime	Session Lifetime	Idle Timeout	Configure
1 Default	guest	7 Days	1 Hour	10 Minutes	 
2 Wireless Guest	guest	7 Days	1 Hour	10 Minutes	 

## Global Guest Settings

Check **Show guest login status window with logout button** to display a user login window on the users's workstation whenever the user is logged in. Users must keep this window open during their login session. The window displays the time remaining in their current session. Users can log out but clicking the **Logout** button in the login status window.



## Guest Profiles

The Guest Profiles list shows the profiles you have created and enables you to add, edit, and delete profiles. **To add a profile:**

**Step 1** Click **Add** below the Guest Profile list to display the Add Guest Profile window.



**Step 2** In the Add Guest Profile window, configure:

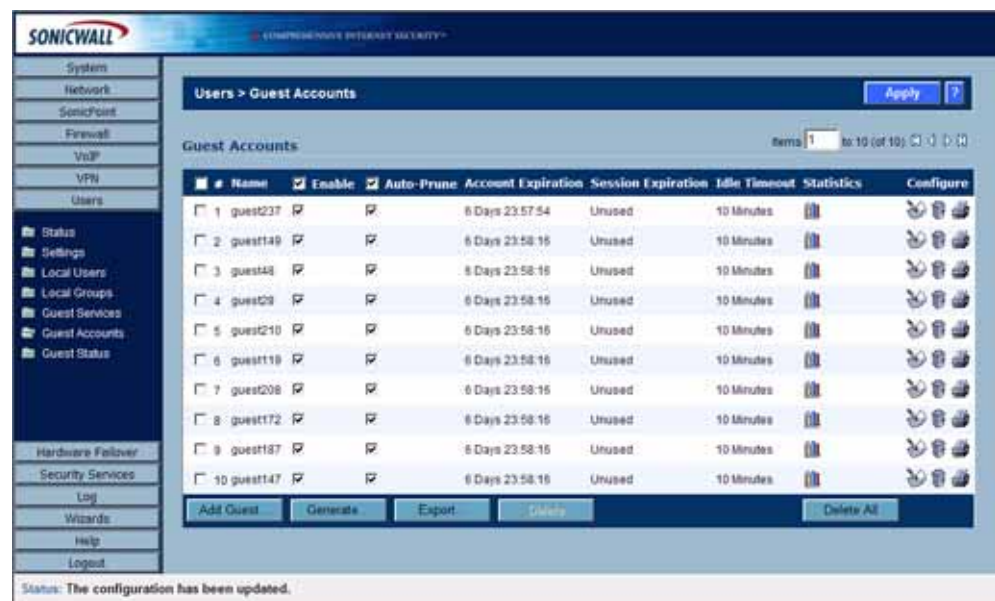
- **Profile Name:** Enter the name of the profile.
- **User Name Prefix:** Enter the first part of every user account name generated from this profile.
- **Auto-generate user name:** Check this to allow guest accounts generated from this profile to have an automatically generated user name. The user name is usually the prefix plus a two- or three-digit number.
- **Auto-generate password:** Check this to allow guest accounts generated from this profile to have an automatically generated password. The generated password is an eight-character unique alphabetic string.
- **Enable Account:** Check this for all guest accounts generated from this profile to be enabled upon creation.

- **Auto-Prune Account:** Check this to have the account removed from the database after its lifetime expires.
- **Enforce login uniqueness:** Check this to allow only a single instance of an account to be used at any one time. By default, this feature is enabled when creating a new guest account. If you want to allow multiple users to login with a single account, disable this enforcement by clearing the Enforce login uniqueness checkbox.
- **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation.
- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**.
- **Comment:** Any text can be entered as a comment in the **Comment** field.

**Step 3** Click **OK** to add the profile.

## Users > Guest Accounts

The **Users > Guest Accounts** page lists the guest services accounts on the security appliance. In the guest services accounts, you can enable or disable individual accounts, groups of accounts, or all accounts, you can set the Auto-Prune feature for accounts, and you can add, edit, delete, and print accounts.

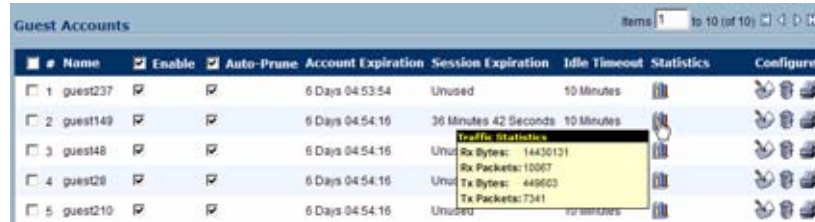


Name	Enable	Auto-Prune	Account Expiration	Session Expiration	Idle Timeout	Statistics	Configure
1 guest237	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:57:54	Unused	10 Minutes		
2 guest149	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
3 guest48	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
4 guest29	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
5 guest210	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
6 guest119	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
7 guest208	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
8 guest172	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
9 guest187	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		
10 guest147	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	8 Days 23:58:15	Unused	10 Minutes		

Status: The configuration has been updated.

## Viewing Guest Account Statistics

To view statistics on a guest account, hover your mouse over the Statistics icon in the line of the guest account. The statistics window will display the cumulative total bytes and packets sent and received for all completed sessions. Currently active sessions will not be added to the statistics until the guest user logs out.



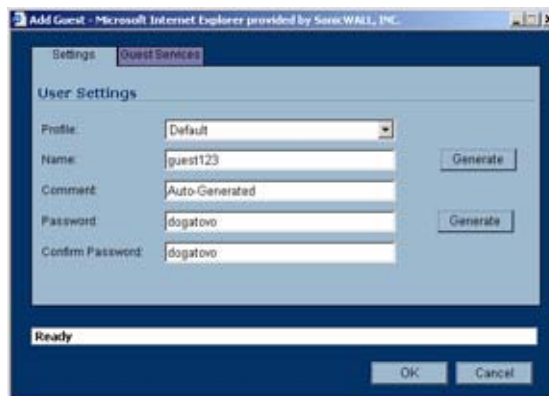
#	Name	Enable	Auto-Prune	Account Expiration	Session Expiration	Idle Timeout	Statistics	Configure
1	guest237	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6 Days 04:53:54	Unused	10 Minutes		
2	guest149	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6 Days 04:54:16	36 Minutes 42 Seconds	10 Minutes	<b>Traffic Statistics</b> Un: Rx Bytes: 14430131 Un: Rx Packets: 10067 Un: Tx Bytes: 449603 Un: Tx Packets: 7341	
3	guest48	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6 Days 04:54:16	Un:	Un:		
4	guest20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6 Days 04:54:16	Un:	Un:		
5	guest210	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	6 Days 04:54:16	Un:	Un:		

## Adding Guest Accounts

You can add guest accounts individually or generate multiple guest accounts automatically.

### To Add an Individual Account:

**Step 1** Under the list of accounts, click **Add Guest**.



Add Guest - Microsoft Internet Explorer provided by SonicWall, Inc.

Settings Guest Services

User Settings

Profile: Default

Name: guest123

Comment: Auto-Generated

Password: dogatovo

Confirm Password: dogatovo

Ready

**Step 2** In the **Settings** tab of the Add Guest Account window configure:

- **Profile:** Select the Guest Profile to generate this account from.
- **Name:** Enter a name for the account or click **Generate**. The generated name is the prefix in the profile and a random two or three digit number.
- **Comment:** Enter a descriptive comment.
- **Password:** Enter the user account password or click **Generate**. The generated password is a random string of eight alphabetic characters.
- **Confirm Password:** If you did not generate the password, re-enter it.



#### Note

Make a note of the password. Otherwise you will have to reset it.

**Step 3** In the **Guest Services** tab, configure:

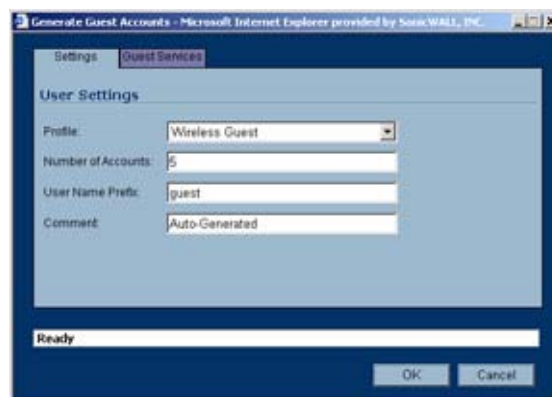


- **Enable Guest Services Privilege:** Check this for the account to be enabled upon creation.
- **Enforce login uniqueness:** Check this to allow only one instance of this account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires.
- **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

**Step 4** Click **OK** to generate the account.

## To Generate Multiple Accounts

**Step 1** Under the list of accounts, click **Generate**.



**Step 2** In the **Settings** tab of the Generate Guest Accounts window configure:

- **Profile:** Select the Guest Profile to generate the accounts from.
- **Number of Accounts:** Enter the number of accounts to generate.
- **User Name Prefix:** Enter the prefix from which account names are generated. For example, if you enter **Guest** the generated accounts will have names like “Guest 123” and “Guest 234”.

- **Comment:** Enter a descriptive comment.

**Step 3** In the **Guest Services** tab, configure:

- **Enable Guest Services Privilege:** Check this for the accounts to be enabled upon creation.
- **Enforce login uniqueness:** Check this to allow only one instance of each generated account to log into the security appliance at one time. Leave it unchecked to allow multiple users to use this account at once.
- **Automatically prune account upon account expiration:** Check this to have the account removed from the database after its lifetime expires.
- **Account Lifetime:** This setting defines how long an account remains on the security appliance before the account expires. If **Auto-Prune** is enabled, the account is deleted when it expires. If the **Auto-Prune** checkbox is cleared, the account remains in the list of guest accounts with an **Expired** status, allowing easy reactivation. This setting overrides the account lifetime setting in the profile.
- **Session Lifetime:** Defines how long a guest login session remains active after it has been activated. By default, activation occurs the first time a guest user logs into an account. Alternatively, activation can occur at the time the account is created by clearing the **Activate account upon first login** checkbox. The **Session Lifetime** cannot exceed the value set in the **Account Lifetime**. This setting overrides the session lifetime setting in the profile.
- **Idle Timeout:** Defines the maximum period of time when no traffic is passed on an activated guest services session. Exceeding the period defined by this setting expires the session, but the account itself remains active as long as the **Account Lifetime** hasn't expired. The **Idle Timeout** cannot exceed the value set in the **Session Lifetime**. This setting overrides the idle timeout setting in the profile.

**Step 4** Click **OK** to generate the accounts.

## Enabling Guest Accounts

You can enable or disable any number of accounts at one time. To enable one or more guest accounts:

**Step 1** Check the box in the **Enable** column next to the name of the account you want to enable. Check the **Enable** box in the table heading to enable all accounts on the page.

**Step 2** Click on **Apply** in the top right corner of the page.





## Enabling Auto-prune for Guest Accounts

You can enable or disable auto-prune for any number of accounts at one time. When auto-prune is enabled, the account is deleted after it expires. To enable auto-prune:

**Step 1** Check the box in the **Auto-Prune** column next to the name of the account. Check the **Auto-Prune** box in the table heading to enable it on all accounts on the page.

**Step 2** Click on **Apply** in the top right corner of the page.

## Printing Account Details.

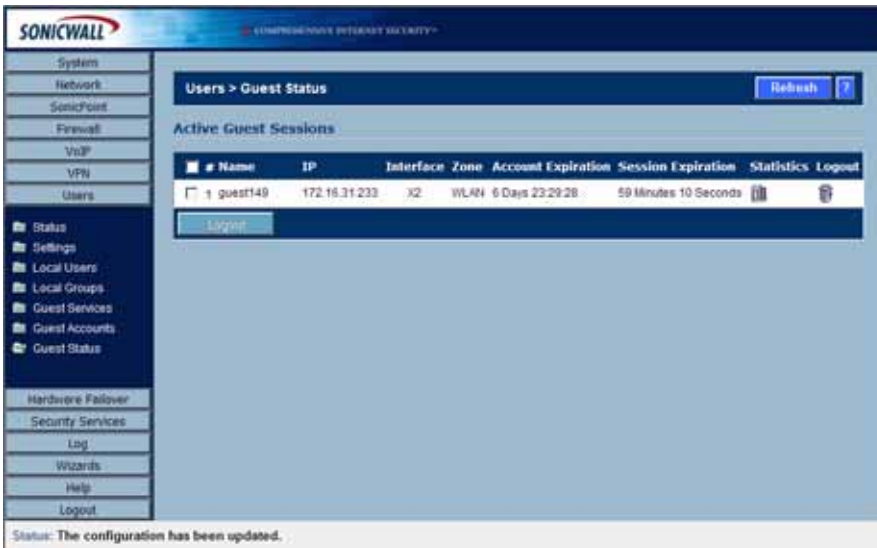
You can print a summary of a guest account. Click the print icon  to launch a summary account report page and send that page to an active printer.





Description	Value
Account Name:	guest141
Password:	prtrtrtr
Enabled:	Yes
Comment:	Auto-Generated
Created:	FRI MAY 28 12:01:08 2004
Account Expires:	FRI JUN 04 12:01:08 2004
Session Expires:	Unused
Session Lifetime:	1 Hour
Idle Timeout:	10 Minutes

## Users > Guest Status

The Guest Status page reports on all the guest accounts currently logged in to the security appliance.



#	Name	IP	Interface	Zone	Account Expiration	Session Expiration	Statistics	Logout
1	guest149	172.16.31.233	X2	WLAN	6 Days 23:29:28	59 Minutes 10 Seconds		

Status: The configuration has been updated.

The page lists:

- **Name:** The name of the guest account.
- **IP:** The IP address the guest user is connecting to.
- **Interface:** The interface on the security appliance through which the user account is connecting to the appliance. For example, If the guest account is a wireless user connecting through a SonicWALL SonicPoint, and all SonicPoints are connecting to the **OPT** port on the appliance, which is configured as a Wireless Zone, the **Interface** column will list **OPT**.
- **Zone:** The Zone on the security appliance that the guest user is connecting to. For example, a wireless user might be connecting to the **WLAN** zone.
- **Account Expiration:** The date, hour, or minute when the account expires.

- **Session Expiration:** The time when the current session expires.
- **Statistics:** hover your mouse over the Statistics icon to view statistics for total received and sent bytes and packets for this guest user's current session.

The screenshot shows a table titled "Active Guest Sessions" with the following columns: #, Name, IP, Interface, Zone, Account Expiration, Session Expiration, Statistics, and Logout. A single row is visible for user "guest149" with IP "172.16.31.233" on interface "X2" in zone "WLAN". The account expiration is "6 Days 23:29:28" and session expiration is "59 Minutes 10 Seconds". A tooltip for the Statistics icon shows the following traffic statistics:

Traffic Statistics	
Rx Bytes:	60948
Rx Packets:	71
Tx Bytes:	703
Tx Packets:	4

- **Logout:** Click the Logout icon to log the guest user off of the security appliance.

Click **Refresh** in the top right of the page at any time to update the information in the list.

## Logging Accounts off the Appliance

As administrator, you can log users off the security appliance:

- To log an individual user out, click the Logout icon in the **Logout** column for that user.
- To log multiple users out, click the checkbox in the first column to select individual users, or check the checkbox next to the **#** in the table heading to select all the guest users listed on the page. Then click **Logout** below the list.

# **PART 11**

# **Security Services**





## CHAPTER 54

# Managing SonicWALL Security Services

---

## SonicWALL Security Services

SonicWALL, Inc. offers a variety of subscription-based security services to provide layered security for your network. SonicWALL security services are designed to integrate seamlessly into your network to provide complete protection.

The following subscription-based security services are listed in **Security Services** on the SonicWALL security appliance's management interface:

- SonicWALL Content Filtering Service
- SonicWALL Client Anti-Virus
- SonicWALL Gateway Anti-Virus\*
- SonicWALL Intrusion Prevention Service\*
- SonicWALL Anti-Spyware\*
- SonicWALL E-Mail Filter\*\*
- SonicWALL Global Security Client



**Note**

---

*Included as part of the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service unified threat management solution. Also included with SonicWALL Client Anti-Virus.*

---



**Tip**

---

After you register your SonicWALL security appliance, you can try FREE TRIAL versions of SonicWALL Content Filtering Service, SonicWALL Client Anti-Virus, SonicWALL Gateway Anti-Virus, SonicWALL Intrusion Prevention Service, and SonicWALL Anti-Spyware.

---

You can activate and manage SonicWALL security services directly from the SonicWALL management interface or from <https://www.mySonicWALL.com>.



**Note** For more information on SonicWALL security services, please visit <http://www.sonicwall.com>.



**Note** Complete product documentation for SonicWALL security services are available on the SonicWALL documentation Web site <http://www.sonicwall.com/us/Support.html>.

## Security Services Summary

The **Security Services > Summary** page lists the available SonicWALL security services and upgrades for your SonicWALL security appliance and provides access to mySonicWALL.com for activating services using Activation Keys.

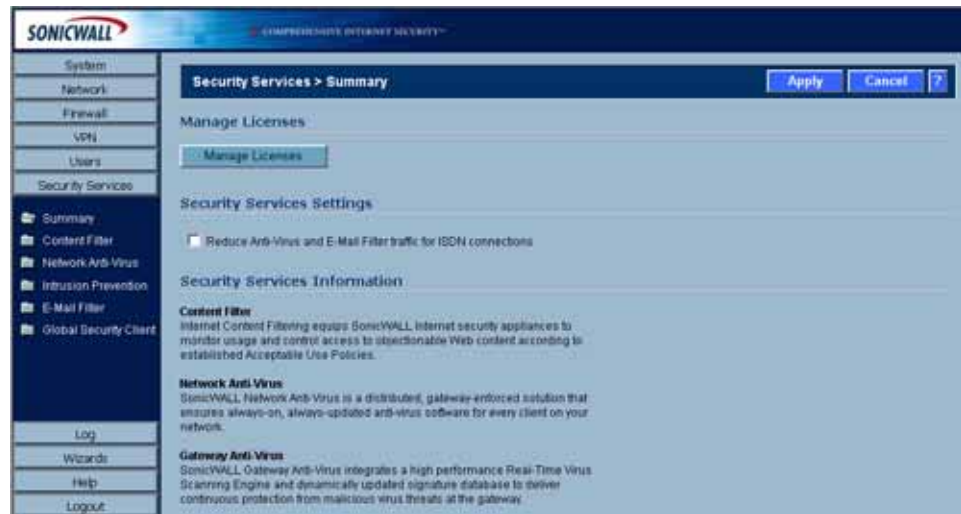
Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Licensed		Renew		07 Apr 2006
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

A list of currently available services is displayed in the **Security Services Summary** table. Subscribed services are displayed with **Licensed** in the **Status** column. The service expiration date is displayed in the **Expiration** column. If the service is limited to a number of users, the number is displayed in the **Count** column. If the service is not licensed, **Not Licensed** is displayed in the **Status** column. If the service license has expired, **Expired** is displayed in the Status column.

When you access your mySonicWALL.com account from this page in the SonicWALL management interface, the **Security Services Summary** table changes to the **Manage Services Online** table. This table provides an updated status of your security services and allows you to activate FREE TRIAL versions, and activate or renew security services licenses using Activation Keys.



If your SonicWALL security appliance is not registered, the **Security Services > Summary** page does not include the **Services Summary** table. Your SonicWALL security appliance must be registered to display the **Services Summary** table.



## mySonicWALL.com

To activate SonicWALL Security Services, you need to have a mySonicWALL.com account and your SonicWALL security appliance must be registered. Creating a mySonicWALL.com account is easy and free. You can create a mySonicWALL.com account directly from the SonicWALL management interface. Simply complete an online registration form. Once your account is created, you can register SonicWALL security appliances and activate SonicWALL Security Services associated with the SonicWALL security appliance.

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL security appliance
- Try free trials of SonicWALL security services
- Purchase/Activate SonicWALL security service licenses
- Receive SonicWALL firmware and security service updates and alerts
- Manage your SonicWALL security services
- Access SonicWALL Technical Support

Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

## Managing Security Services Online

Clicking the **Manage Licenses** button displays the **mySonicWALL.com Login** page for accessing your MySonicWALL.com account licensing information.

mySonicWALL.com Login

mySonicWALL.com is a one-stop resource for registering all your SonicWALL Internet Security Appliances and managing all your SonicWALL security service upgrades and changes. mySonicWALL provides you with an easy to use interface to manage services and upgrades for multiple SonicWALL appliances. For more information on mySonicWALL please visit the [FAQ](#). If you do not have a mySonicWall account, please click [here](#) to create one. Otherwise, please enter your existing mySonicWALL.com username and password below.

User Name:

Password:

Enter your mySonicWALL.com username and password in the **User Name** and **Password** fields, and then click **Submit**. The **System > Licenses** page is displayed with the **Manage Services Online** table.

The information in the **Manage Services Online** table is updated from your mySonicWALL.com account.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway AntiVirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Licensed		Renew		07 Apr 2006
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

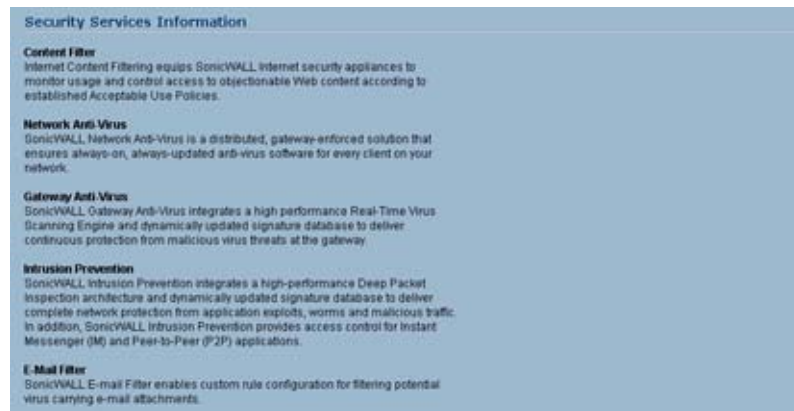
If you are already connected to your mysonicwall.com account from the management interface, the **Manage Services Online** table is displayed.

## Security Services Settings

- **Synchronize** - Click **Synchronize** to update the licensing and subscription information on the SonicWALL security appliance from your mysonicwall.com account.
- **Reduce Anti-Virus and E-mail Filter traffic for ISDN connections** - Selecting this feature enables the SonicWALL Anti-Virus to only check daily (every 24 hours) for updates and reduces the frequency of outbound traffic for users who do not have an “always on” Internet connection.

## Security Services Information

This section includes a brief overview of services available for your SonicWALL security appliance.



## Update Signature Manually

The Manual Signature Update feature is intended for networks where reliable, broadband Internet connectivity is either not possible or not desirable (for security reasons).

The Manual Signature Update feature provides a method to update the latest signatures at the network administrator's discretion. The network administrator first downloads the signatures from <http://www.mysonicwall.com> to a separate computer, a USB drive, or other media. Then the network administrator uploads the signatures to the SonicWALL security appliance.

The same signature update file can be used to all SonicWALL security appliances that meet the following requirements:

- Devices that are registered to the same mysonicwall.com account
- Devices that belong to the same class of SonicWALL security appliances. There are two classes of SonicWALL security appliances:
  - The SonicWALL TZ series and the SonicWALL PRO 1260
  - The SonicWALL PRO series except for the SonicWALL PRO 1260

To manually update signature files, complete the following steps:

- Step 1** On the **Security Services > Summary** page, scroll to the **Update Signatures Manually** heading at the bottom of the page. Note the Signature File ID for the device.

The screenshot shows the SonicWALL Security Services Summary page. The left sidebar contains a navigation menu with the following items: System, Network, Firewall, VPN, Users, Security Services, Summary (selected), Content Filter, Network Anti-Virus, Gateway Anti-Virus, Intrusion Prevention, Anti-Spyware, and E-Mail Filter. Below the sidebar are buttons for Log, Wizards, Help, and Logout. The main content area displays the following information:

- System:** SonicWALL Gateway Anti-Virus integrates a high performance Real-Time Virus Scanning Engine and dynamically updated signature database to deliver continuous protection from malicious virus threats at the gateway.
- Anti-Spyware:** SonicWALL Anti-Spyware prevents malicious spyware from infecting networks by blocking spyware installation at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.
- Intrusion Prevention:** SonicWALL Intrusion Prevention integrates a high-performance Deep Packet Inspection architecture and dynamically updated signature database to deliver complete network protection from application exploits, worms and malicious traffic. In addition, SonicWALL Intrusion Prevention provides access control for Instant Messenger (IM) and Peer-to-Peer (P2P) applications.
- E-Mail Filter:** SonicWALL E-mail Filter enables custom rule configuration for filtering potential virus carrying e-mail attachments.

The **Update signatures manually** section is highlighted and contains a text box for **Signature File ID:** with the value **2** entered. Below this text box is a note: "If you work in a closed environment or prefer to update AV signatures manually, please download signature updates from [mySonicWALL.com](http://www.mysonicwall.com) to your disk, then import the file." At the bottom of this section is an **Import Signatures** button.

- Step 2** Log on to <http://www.mysonicwall.com> using the mysonicwall.com account that was used to register the SonicWALL security appliance.

**Note**

The signature file can only be used on SonicWALL security appliances that are registered to the mysonicwall.com account that downloaded the signature file.

**Step 3** Click on **Download Signatures** under the **Downloads** heading.

The screenshot shows the SonicWALL mySonicWALL 3.6.11.0 interface. The top navigation bar includes the SonicWALL logo and the text 'COMPREHENSIVE INTERNET SECURITY™'. Below this, the user is logged in as 'teSt' with a 'LOGOUT' button. The main content area is titled 'Download Signature Files' and contains a message: 'Download Signature Files based on the Signature File Id for your Product. This feature is available only when running SonicOS Enhanced version 3.2 or newer.' There are two pull-down menus: 'Signature ID:' set to '3' and 'Applicable Products:' with options 'PRO 1260', 'PRO 2040', and 'PRO 4060'. Under the 'Available Download' section, there is a link: 'Click here to download the Signature File'. The left sidebar contains various navigation options: Home, My Products, My Account, Personal Info, Preferences, My Orders (View Cart, Auto-Renewal, Co termination, Order History), Reports, Downloads (Download Center, My Downloads, Download Signatures), Support (Feedback, Service Requests, Forum), My Training, My Promotions, and Quick Register.

**Step 4** In the pull down window next to **Signature ID:**, select the appropriate SFID for your SonicWALL security appliance.

**Step 5** Download the signature update file by clicking on **Click here to download the Signature file.**

**Note**

The remaining steps can be performed while disconnected from the Internet.

**Step 6** Return to the Security Services > Summary page on the SonicWALL security appliance GUI.

**Step 7** Click on the **Import Signatures** box.

**Step 8** In pop-up window that appears, click the **browse** button, and navigate to the location of the signature update file.

**Step 9** Click **Import**. The signatures are uploaded for the security services that are enabled on the SonicWALL security appliance.

## Activating Security Services

To activate a SonicWALL Security Service FREE TRIAL or activate a license using an Activation Key, refer to the specific SonicWALL Security Service chapter in this guide.



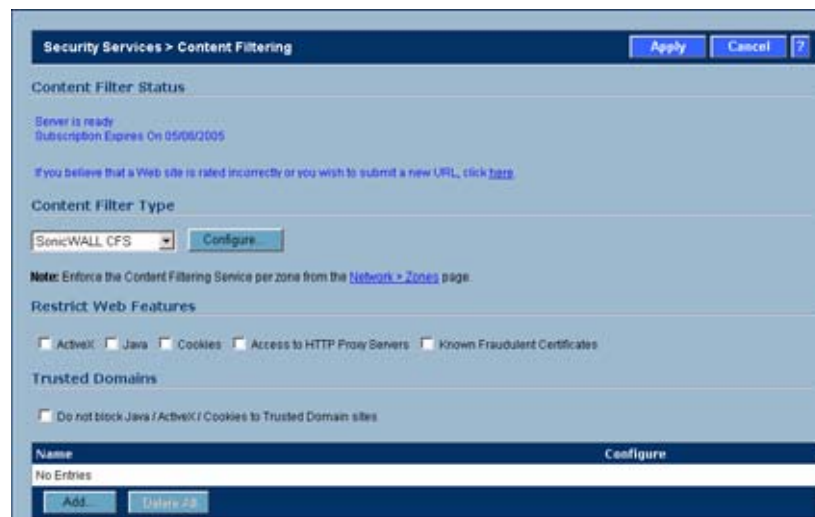


## CHAPTER 55

# Configuring SonicWALL Content Filtering Service

## Security Services > Content Filter

The **Security Services > Content Filter** page allows you to configure the SonicWALL Restrict Web Features and Trusted Domains settings, which are included with SonicOS Enhanced. You can activate and configure SonicWALL Content Filtering Service (SonicWALL CFS) as well as two third-party Content Filtering products from the **Security Services > Content Filter** page.



Security Services > Content Filtering [Apply] [Cancel] [?]

Content Filter Status

Server is ready  
Subscription Expires On 05/06/2005

If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click [here](#).

Content Filter Type

SonicWALL CFS [Configure]

**Note:** Enforce the Content Filtering Service per zone from the [Network > Zones](#) page.

Restrict Web Features

ActiveX  Java  Cookies  Access to HTTP Proxy Servers  Known Fraudulent Certificates

Trusted Domains

Do not block Java / ActiveX / Cookies to Trusted Domain sites

Name	Configure
No Entries	

[Add] [Delete 23]



*SonicWALL Content Filtering Service is a subscription service upgrade. You can try a FREE TRIAL of SonicWALL directly from your SonicWALL management interface. See “Activating a SonicWALL CFS FREE TRIAL” on page 697.*

For complete SonicWALL Content Filtering Service documentation, see the SonicWALL Content Filtering Service Standard or Premium Administrator’s Guide available at <http://www.sonicwall.com/us/Support.html>.

## SonicWALL Content Filtering Service

SonicWALL Content Filtering Service (CFS) enforces protection and productivity policies for businesses, schools and libraries to reduce legal and privacy risks while minimizing administration overhead. SonicWALL CFS utilizes a dynamic database of millions of URLs, IP addresses and domains to block objectionable, inappropriate or unproductive Web content. At the core of SonicWALL CFS is an innovative rating architecture that cross references all Web sites against the database at worldwide SonicWALL co-location facilities. A rating is returned to the SonicWALL security appliance and then compared to the content filtering policy established by the administrator. Almost instantaneously, the Web site request is either allowed through or a Web page is generated by the SonicWALL security appliance informing the user that the site has been blocked according to policy.

With SonicWALL CFS, network administrators have a flexible tool to provide comprehensive filtering based on keywords, time of day, trusted and forbidden domain designations, and file types such as Cookies, Java™ and ActiveX® for privacy. SonicWALL CFS automatically updates the filters, making maintenance substantially simpler and less time consuming.

SonicWALL CFS can also be customized to add or remove specific URLs from the blocked list and to block specific keywords. When a user attempts to access a site that is blocked by the SonicWALL security appliance, a customized message is displayed on the user's screen. SonicWALL security appliance can also be configured to log attempts to access sites on the SonicWALL Content Filtering Service database, on a custom URL list, and on a keyword list to monitor Internet usage before putting new usage restrictions in place.

- **SonicWALL CFS Standard** blocks 12 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Standard runs on SonicOS Standard 2.0 (or higher).
- **SonicWALL CFS Premium** blocks 56 categories of objectionable, inappropriate or unproductive Web content. SonicWALL CFS Premium provides network administrators with greater control by automatically and transparently enforces acceptable use policies. It gives administrators the flexibility to enforce custom content filtering policies for groups of users on the network. For example, a school can create one policy for teachers and another for students. SonicWALL CFS Premium Productivity Edition and the SonicWALL CFS Premium Government/Education Edition run on SonicOS Standard 2.1 (or higher) as well as SonicOS Enhanced 2.0 (or higher).



### Note

For complete SonicWALL Content Filtering Service documentation, see the SonicWALL Content Filtering Service Administrator's Guide available at <http://www.sonicwall.com/us/Support.html>

## Content Filter Status

If SonicWALL CFS is activated, the **Content Filter Status** section displays the status of the Content Filter Server, as well as the date and time that your subscription expires. The expiration date and time is displayed in Universal Time Code (UTC) format.





You can also access the **SonicWALL CFS URL Rating Review Request** form by clicking on the **here** link in **If you believe that a Web site is rated incorrectly or you wish to submit a new URL, click here.**

If SonicWALL CFS is not activated, you must activate it. If you do not have an Activation Key, you must purchase SonicWALL CFS from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).

## Activating SonicWALL CFS

If you have an Activation Key for your SonicWALL CFS subscription, follow these steps to activate SonicWALL CFS:



Warning

---

**You must have a mySonicWALL.com account and your SonicWALL security appliance must be registered to activate SonicWALL Client Anti-Virus.**

---

- Step 1** Click the **SonicWALL Content Filtering Subscription** link on the **Security Services > Content Filtering** page. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL CFS subscription is activated on your SonicWALL.
- Step 4** If you activated SonicWALL CFS at mySonicWALL.com, the SonicWALL CFS activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL.

## Activating a SonicWALL CFS FREE TRIAL

You can try a FREE TRIAL of SonicWALL CFS by following these steps:

- Step 1** Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- Step 3** Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL CFS trial subscription is activated on your SonicWALL.
- Step 4** Select **Security Services > Content Filter** to display the Content Filter page for configuring your SonicWALL Content Filtering Service settings.

## Content Filter Type

There are three types of content filtering available on the SonicWALL security appliance. These options are available from the **Content Filter Type** menu.

- **SonicWALL CFS** - Selecting **SonicWALL CFS** as the **Content Filter Type** allows you to use the SonicWALL Content Filtering Service that is available as an upgrade. You can obtain more information about SonicWALL Content Filtering Service at <http://www.sonicwall.com/products/cfs.html>
- **N2H2** - N2H2 is a third party content filter software package supported by SonicWALL security appliance.
- **Websense Enterprise** - Websense Enterprise is also a third party content filter list supported by SonicWALL security appliance.

Clicking the **Network > Zones** link in **Note: Enforce the Content Filtering per zone from the Network > Zone page**, displays the **Network > Zones** page for enabling SonicWALL Content Filtering Service on network zones.

## Restrict Web Features

**Restrict Web Features** enhances your network security by blocking potentially harmful Web applications from entering your network.

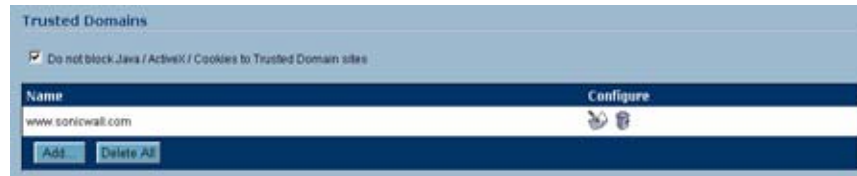


**Restrict Web Features** are included with SonicOS. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the **ActiveX** check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the **Java** check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the **Cookies** check box to disable Cookies.
- **Access to HTTP Proxy Servers** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL security appliance blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL security appliance include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

## Trusted Domains

Trusted Domains can be added to enable content from specific domains to be exempt from **Restrict Web Features**.



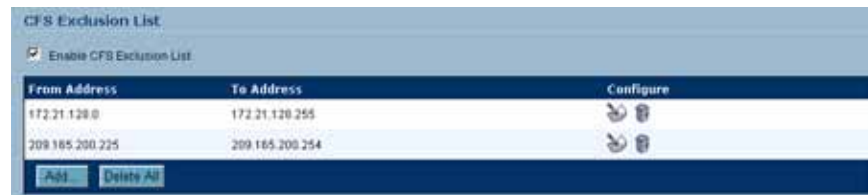
If you trust content on specific domains and want them exempt from **Restrict Web Features**, follow these steps to add them:

- 
- Step 1** Check the **Don't block Java/ActiveX/Cookies to Trusted Domains** checkbox.
  - Step 2** Click **Add**. The **Add Trusted Domain Entry** window is displayed.
  - Step 3** Enter the trusted domain name in the **Domain Name** field.
  - Step 4** Click **OK**. The trusted domain entry is added to the Trusted Domain table.

To keep the trusted domain entries but enable Restrict Web Features, uncheck **Don't block Java/ActiveX/Cookies to Trusted Domains**. To delete an individual trusted domain, click on the **Trashcan** icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Notepad** icon.

## CFS Exclusion List

IP address ranges can be manually added to the CFS Exclusion List.

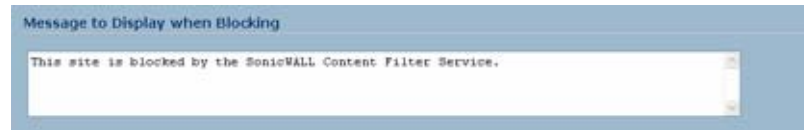


To manually add a range of IP addresses to the CFS Exclusion List, follow these steps:

- 
- Step 1** Check the **Enable CFS Exclusion List** checkbox.
  - Step 2** Click **Add**. The **Add CFS Range Entry** window is displayed.
  - Step 3** Enter the first IP address in the range in the **IP Address From:** field and the last address in the **IP Address To:** field.
  - Step 4** Click **OK**. The IP address range is added to the CFS Exclusion List.
  - Step 5** To keep the CFS Exclusion List entries but temporarily allow access to these sites, uncheck the **Enable CFS Exclusion List** checkbox. To delete an individual trusted domain, click on the **Trashcan** icon for the entry. To delete all trusted domains, click **Delete All**. To edit a trusted domain entry, click the **Notepad** icon.

## Message to Display when Blocking

You can enter your customized text to display to the user when access to a blocked site is attempted. The default message is **This site is blocked by the SonicWALL Content Filter Service**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.

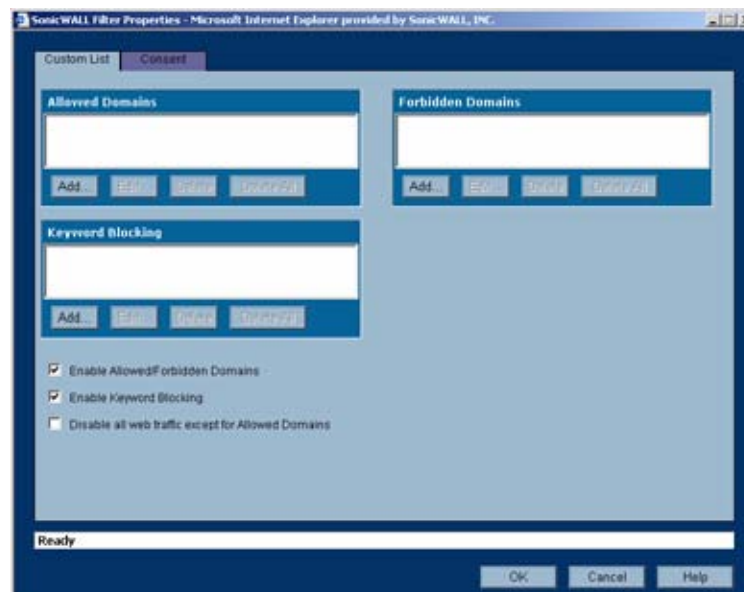


## Configuring SonicWALL Filter Properties

You can customize SonicWALL filter features included with SonicOS from the **SonicWALL Filter Properties** window. To display the **SonicWALL Filter Properties** window, select **SonicWALL CFS** from the **Content Filter Type** menu on the **Security Services > Content Filter** page, and click **Configure**. The **SonicWALL Filter Properties** window is displayed.

## Custom List

You can customize your URL list to include **Allowed Domains** and **Forbidden Domains**. By customizing your URL list, you can include specific domains to be accessed, blocked, and include specific keywords to block sites. Select the check box **Enable Allowed/Forbidden Domains** to activate this feature.



To allow access to a Web site that is blocked by the Content Filter List, click **Add**, and enter the host name, such as “www.ok-site.com”, into the Allowed Domains fields. 256 entries can be added to the **Allowed Domains** list.

To block a Web site that is not blocked by the **Content Filter Service**, click **Add**, and enter the host name, such as “www.bad-site.com” into the **Forbidden Domains** field. 256 entries can be added to the **Forbidden Domains** list.



Warning

Do not include the prefix “http://” in either the **Allowed Domains** or **Forbidden Domains** the fields. All subdomains are affected. For example, entering “yahoo.com” applies to “mail.yahoo.com” and “my.yahoo.com”.

To remove a trusted or forbidden domain, select it from the appropriate list, and click **Delete**. Once the domain has been deleted, the **Status** bar displays **Ready**.

## Enable Keyword Blocking

To enable blocking using **Keywords**, select **Enable Keyword Blocking**. Click **Add**, and enter the keyword to block in the **Add Keyword** field, and click **OK**.

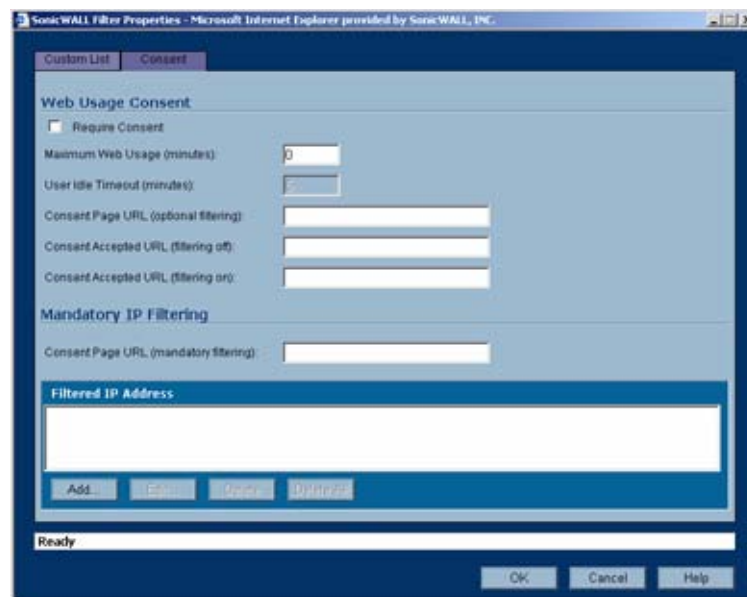
To remove a keyword, select it from the list and click **Delete**. Once the keyword has been removed, the **Status** bar displays **Ready**.

## Disable all Web traffic except for Allowed Domains

When the **Disable Web traffic except for Allowed Domains** check box is selected, the SonicWALL security appliance only allows Web access to sites on the **Allowed Domains** list. With careful screening, this can be nearly 100% effective at blocking pornography and other objectionable material.

## Consent

The **Consent** tab allows you to enforce content filtering on designated computers and provide optional filtering on other computers. Consent can be configured to require the user to agree to the terms outlined in an **Acceptable Use Policy** window before Web browsing is allowed.



To enable the **Consent** properties, select **Require Consent**.

- **Maximum Web Usage (minutes)** - In an environment where there are more users than computers, such as a classroom or library, time limits are often imposed. The SonicWALL security appliance can be used to remind users when their time has expired by displaying

the page defined in the **Consent** page URL field. Enter the time limit, in minutes, in the **Maximum Web usage** field. When the default value of zero (0) is entered, this feature is disabled.

- **User Idle Timeout (minutes)** - After a period of Web browser inactivity, the SonicWALL security appliance requires the user to agree to the terms outlined in the Consent page before accessing the Internet again. To configure the value, follow the link to the Users window and enter the desired value in the User Idle Timeout section.
- **Consent Page URL (optional filtering)** - When a user opens a Web browser on a computer requiring consent, they are shown a consent page and given the option to access the Internet with or without content filtering. This page must reside on a Web server and be accessible as a URL by users on the network. It can contain the text from, or links to an Acceptable Use Policy (AUP). This page must contain links to two pages contained in the SonicWALL security appliance, which, when selected, tell the SonicWALL security appliance if the user wishes to have filtered or unfiltered access. The link for unfiltered access must be <192.168.168.168/iAccept.html> and the link for filtered access must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168".
- **Consent Accepted URL (filtering off)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet without the protection of **Content Filtering**, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering off)** field. This page must reside on a Web server and be accessible as a URL by users on the network.
- **Consent Accepted URL (filtering on)** - When a user accepts the terms outlined in the **Consent** page and chooses to access the Internet with the protection of Content Filtering, they are shown a Web page confirming their selection. Enter the URL of this page in the **Consent Accepted (filtering on)** field. This page must reside on a Web server and be accessible as a URL by users on the network.

## Mandatory Filtered IP Addresses

When a user opens a Web browser on a computer using mandatory content filtering, a consent page is displayed. You must create the Web page that appears when the Web browser is opened. It can contain text from an Acceptable Use Policy, and notification that violations are logged or blocked.

This Web page must reside on a Web server and be accessible as a URL by users on the LAN. This page must also contain a link to a page contained in the SonicWALL security appliance that tells the device that the user agrees to have filtering enabled. The link must be <192.168.168.168/iAcceptFilter.html>, where the SonicWALL LAN IP Address is used instead of 192.168.168.168.

Enter the URL of this page in the **Consent Page URL (mandatory filtering)** field and click **OK**. Once the SonicWALL security appliance has been updated, a message confirming the update is displayed at the bottom of the Web browser window.

## Adding a New Address

The SonicWALL security appliance can be configured to enforce content filtering for certain computers on the LAN. Click **Add** to display the **Add Filtered IP Address Entry** window. Enter the IP addresses of these computers in the **Add New Address** field and click **Submit** button. Up to 128 IP addresses can be entered.

To remove a computer from the list of computers to be filtered, highlight the IP address in the **Mandatory Filtered IP Addresses** list and click **Delete**.

## Configuring N2H2 Internet Filtering

N2H2 is a third party Internet filtering package that allows you to use Internet content filtering through the SonicWALL.

- 
- Step 1** Select **N2H2** from the **Content Filter Type** list.
- Step 2** Click **Configure** to display the **N2H2 Properties** window.



**Note** You specify enforcement of content filtering on the **Network > Zones** page.

---

## N2H2 Properties

The **General** page includes the following settings. After configuring N2H2 content filtering in the N2H2 Properties window, click **OK**.

## N2H2 Server Status

This section displays the status of the N2H2 Internet Filtering Protocol (IFP) server you are using for Internet filtering.

## Settings

- **Server Host Name or IP Address** - Enter the Server Host Name or the IP address of the N2H2 Internet Filtering Protocol (IFP) server used to receive IFP requests.
- **Listen Port** - Enter the UDP port number for the N2H2 Internet Filtering Protocol (IFP) server to “listen” for the N2H2 traffic. The default port is 4005.
- **Reply Port** - Enter the UCP port number for the N2H2 server to send packets from the N2H2 client to the SonicWALL. The default port is 4005.
- **User Name** - The User Name refers to a configuration of users, a group of users, or network defined within the N2H2 software.
- **If Server is unavailable for (seconds)** - Defines what action is taken if the N2H2 server is unavailable. The default value for timeout of the server is 5 seconds, but you can enter a value between 1 and 10 seconds.
  - **Block traffic to all Web sites** - Selecting this option blocks traffic to all Web sites except Allowed Domains until the N2H2 server is available.
  - **Allow traffic to all Web sites** - Selecting this option allows traffic to all Web sites without N2H2 server filtering. However, Forbidden Domains and Keywords, if enabled, are still blocked.
- **If Server marks URL as blocked** - If the N2H2 server becomes unavailable, select from the following two options:
  - **Block Access to URL** - If this check box is selected, the SonicWALL logs and then blocks access. The SonicWALL also logs attempts to access these sites.
  - **Log Access to URL** - Select the check box and the SonicWALL allows access to blocked URLs but logs access activities.

## URL Cache

- **Cache Size (KB)** - Configure the size of the URL Cache in KB for the SonicWALL.



Tip

**Tip!** A larger URL Cache size can provide noticeable improvements in Internet browsing response times.

## Configuring SonicWALL Blocking Features

Once you configure your settings in the N2H2 Properties window, you can configure SonicWALL blocking features including **Restrict Web Features**, **Trusted Domains**, and **Message to Display when Blocking** from the **Security Services > Content Filtering** page.

### Restrict Web Features

**Restrict Web Features** enhances your network security by blocking potentially harmful Web applications from entering your network. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the ActiveX check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the Java check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the Cookies check box to disable Cookies.
- **Web Proxy** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

### Trusted Domains

**Trusted Domains** can be added in the **Restrict Web Features** section. If you trust content on specific domains, you can select **Don't block Java/ActiveX/Cookies to Trusted Domains** and then add the **Trusted Domains** to the SonicWALL by clicking on **Add**. The **Add Trusted Domain Entry** window appears for entering the trusted domain name.

**Don't Block Java/ActiveX/Cookies to Trusted Domains** - Select this option if you have trusted domains using Java, ActiveX, and Cookies. To add a trusted domain, enter the domain name into the Add Trusted Domain field. Click **OK** to add the domain to the list of trusted domains. To delete a domain, select it from the list, and then click Delete.



## Message to Display when Blocking

You can enter your customized text in the **Message to Display when Blocking** text box that displays to the user when access to a blocked site is attempted. The default message is **The site is blocked by the SonicWALL Content Filter Service**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.

## Configuring Websense Enterprise Content Filtering

Websense Enterprise is a third party Internet filtering package that allows you to use Internet content filtering through the SonicWALL.

- 
- Step 1** Select **Websense Enterprise** from the **Content Filter Type** list.
- Step 2** Click **Configure** to display the **Websense Properties** window.




---

**Note!** You specify enforcement of content filtering on the **Network > Zones** page.

---

## Websense Properties

The **General** page in the **Websense Properties** window includes the following settings. After configuring Websense content filtering in the **Websense Properties** window, click **OK**.

### Websense Server Status

This section displays the status of the Websense Enterprise server used for content filtering.

### Settings

- **Server Host Name or IP Address** - Enter the Server Host Name or the IP address of the Websense Enterprise server used for the Content Filter List.
- **Server Port** - Enter the UDP port number for the SonicWALL to “listen” for the Websense Enterprise traffic. The default port number is 15868.
- **User Name** - To enable reporting of users and groups defined on the Websense Enterprise server, leave this field blank. To enable reporting by a specific user or group behind the SonicWALL, enter the User Name configured on the Websense Enterprise Server for the user or group. If using NT-based directories on the Websense Enterprise Server, the User Name is in this format, for example: NTLM:\\domainname\username. If using LDAP-based directories on the Websense Enterprise server, the User Name is in this format, for example: LDAP://o-domain/ou=sales/username.



**Warning**

---

**Alert!** If you are not sure about the entering a user name in this section, leave the field blank and consult your Websense documentation for more information.

---

- **If Server is unavailable for (seconds)** - Defines what action is taken if the N2H2 server is unavailable. The default value for timeout of the server is 5 seconds, but you can enter a value between 1 and 10 seconds.

- **Block traffic to all Web sites** - Selecting this option blocks traffic to all Web sites except Allowed Domains until the N2H2 server is available.
- **Allow traffic to all Web sites** - Selecting this option allows traffic to all Web sites without Websense Enterprise server filtering. However, Forbidden Domains and Keywords, if enabled, are still blocked.

## URL Cache

- **Cache Size (KB)** - Configure the size of the URL Cache in KB.



Tip

---

**Tip!** A larger URL Cache size can result in noticeable improvements in Internet browsing response times.

---

## Configuring SonicWALL Blocking Features

Once you configure your settings in the Websense Properties window, you can configure SonicWALL blocking features including **Restrict Web Features**, **Trusted Domains**, and **Message to Display when Blocking** from the **Security Services>Content Filtering** page.

### Restrict Web Features

**Restrict Web Features** enhances your network security by blocking potentially harmful Web applications from entering your network. Select any of the following applications to block:

- **ActiveX** - ActiveX is a programming language that embeds scripts in Web pages. Malicious programmers can use ActiveX to delete files or compromise security. Select the ActiveX check box to block ActiveX controls.
- **Java** - Java is used to download and run small programs, called applets, on Web sites. It is safer than ActiveX since it has built-in security mechanisms. Select the Java check box to block Java applets from the network.
- **Cookies** - Cookies are used by Web servers to track Web usage and remember user identity. Cookies can also compromise users' privacy by tracking Web activities. Select the Cookies check box to disable Cookies.
- **Web Proxy** - When a proxy server is located on the WAN, LAN users can circumvent content filtering by pointing their computer to the proxy server. Check this box to prevent LAN users from accessing proxy servers on the WAN.
- **Known Fraudulent Certificates** - Digital certificates help verify that Web content and files originated from an authorized party. Enabling this feature protects users on the LAN from downloading malicious programs warranted by these fraudulent certificates. If digital certificates are proven fraudulent, then the SonicWALL blocks the Web content and the files that use these fraudulent certificates. Known fraudulent certificates blocked by SonicWALL include two certificates issued on January 29 and 30, 2001 by VeriSign to an impostor masquerading as a Microsoft employee.

## Trusted Domains

**Trusted Domains** can be added in the **Restrict Web Features** section. If you trust content on specific domains, you can select **Don't block Java/ActiveX/Cookies to Trusted Domains** and then add the **Trusted Domains** to the SonicWALL by clicking on **Add**. The **Add Trusted Domain Entry** window appears for entering the trusted domain name.

**Don't Block Java/ActiveX/Cookies to Trusted Domains** - Select this option if you have trusted domains using Java, ActiveX, and Cookies. To add a trusted domain, enter the domain name into the Add Trusted Domain field. Click **OK** to add the domain to the list of trusted domains. To delete a domain, select it from the list, and then click Delete.

## Message to Display when Blocking

You can enter your customized text in the **Message to Display when Blocking** text box that displays to the user when access to a blocked site is attempted. The default message is **The site is blocked by the SonicWALL Content Filter Service**. Any message, including embedded HTML, up to 255 characters long, can be entered in this field.





## CHAPTER 56

# Activating SonicWALL Client Anti-Virus

---

## Security Services > Anti-Virus

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses don't have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as NIMDA and Code Red, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Client Anti-Virus prevents occurrences like these and offers a new approach to virus protection. SonicWALL security appliance constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user's computer. In addition, the SonicWALL security appliance restricts each user's access to the Internet until they are protected, therefore acting as an enforcer of the company's virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak.

**Note**

---

You must purchase an Anti-Virus subscription to enforce Anti-Virus through the SonicWALL security appliance's Management Interface.

---

## Activating SonicWALL Client Anti-Virus

If Sonic WALL Client Anti-Virus is not activated, you must activate it.



If you do not have an Activation Key, you must purchase SonicWALL Client Anti-Virus from a SonicWALL reseller or from your mySonicWALL.com account (limited to customer in the USA and Canada).



### Note

For complete SonicWALL Client Anti-Virus documentation, see the SonicWALL Client Anti-Virus Administrator's Guide available at <http://www.sonicwall.com/us/Support.html>

If you have an Activation Key for your SonicWALL Client Anti-Virus subscription, follow these steps to activate SonicWALL Client Anti-Virus:



**Note** You must have a mySonicWALL.com account and your SonicWALL must be registered to activate SonicWALL Client Anti-Virus.

- Step 1** Click the **SonicWALL Client Anti-Virus Subscription** link on the **Security Services > Anti-Virus** page. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Client Anti-Virus Subscription** link.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**. Your SonicWALL Client Anti-Virus subscription is activated on your SonicWALL security appliance.



- Step 4** If you activated SonicWALL Client Anti-Virus at www.mySonicWALL.com, the SonicWALL Client Anti-Virus activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL security appliance.

## Activating a SonicWALL Client Anti-Virus FREE TRIAL

You can try a FREE TRIAL of SonicWALL Client Anti-Virus by following these steps:

- Step 1** Click the **FREE TRIAL** link. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- Step 3** Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL Client Anti-Virus subscription is activated on your SonicWALL security appliance.
- Step 4** Select **Security Services > Anti-Virus** to display the Anti-Virus page for configuring your SonicWALL Client Anti-Virus settings.



## Configuring Client Anti-Virus Service

### Anti-Virus Policies

The following features are available in the Anti-Virus Policies section:

- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted Zones. Choosing this option allows computers on a trusted zone (such as a LAN) to access computers on public zones (such as DMZ), even if anti-virus software is not installed on the LAN computers.
- **Days before forcing update** - This feature defines the maximum number of days may access the Internet before the SonicWALL requires the latest virus date files to be downloaded.
- **Force update on alert** - SonicWALL, Inc. broadcasts virus alerts to all SonicWALL appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the Maximum number of days allowed before forcing update selection. In addition, every virus alert is logged, and an alert message is sent to the administrator.



- **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.
- **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.
- **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

## Anti-Virus Enforcement

SonicWALL Client Anti-Virus currently supports Windows 95, 98, NT, XP, and 2000 platforms. In order to access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement. There are three options for defining exempt computers:

- **Enforce Anti-Virus policies for all computers** - Selecting this option forces computers to install VirusScan ASaP in order to access the Internet or the DMZ. This is the default configuration.
- **Include specified address range in the Anti-Virus enforcement** - Choosing this option allows the administrator to define ranges of IP addresses to receive Anti-Virus enforcement. If you select this option, specify a range of IP addresses to be enforced. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered for enforcement. Click **Add** to display the **Add AV Range Entry** window and then enter the IP address range.
- **Exclude specified address range in the Anti-Virus enforcement** - Selecting this option allows the administrator to define ranges of IP addresses that are exempt from Anti-Virus enforcement. If you select this option, specify the range of IP addresses that are exempt. Any computer requiring unrestricted Internet access needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered. Click **Add** to display the **Add AV Range Entry** window and then enter the IP address range.

## Security Services > E-mail Filter

The **E-Mail Filter** allows the administrator to selectively delete or disable inbound e-mail attachments as they pass through the SonicWALL security appliance. This feature provides control over executable files and scripts, and applications sent as e-mail attachments.

**Note**

E-Mail Filter is included with the Client Anti-Virus service subscription. When you activate SonicWALL Client Anti-Virus, E-Mail Filter is automatically activated.

For complete SonicWALL Client Anti-Virus documentation including E-Mail Filter, see the SonicWALL Client Anti-Virus Administrator's Guide available at <http://www.sonicwall.com/us/Support.html>.



## CHAPTER 57

# Chapter 57: Managing SonicWALL Gateway Anti-Virus Service

---

## Security Services > Gateway Anti-Virus

SonicWALL GAV delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

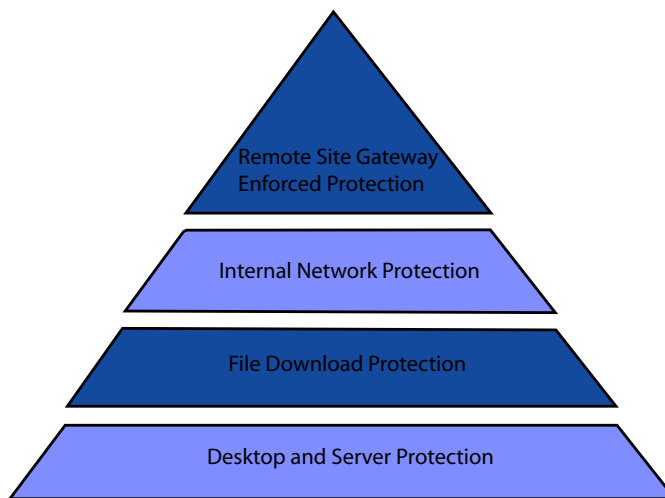
SonicWALL GAV delivers real-time virus protection directly on the SonicWALL security appliance by using SonicWALL's IPS-Deep Packet Inspection v2.0 engine to inspect all traffic that traverses the SonicWALL gateway. Building on SonicWALL's reassembly-free architecture, SonicWALL GAV inspects multiple application protocols, as well as generic TCP streams, and compressed traffic. Because SonicWALL GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding, ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a single-pass, per-packet basis.

SonicWALL GAV delivers threat protection directly on the SonicWALL security appliance by matching downloaded or e-mailed files against an extensive and dynamically updated database of threat virus signatures. Virus attacks are caught and suppressed before they travel to desktops. New signatures are created and added to the database by a combination of SonicWALL's SonicAlert Team, third-party virus analysts, open source developers and other sources.

SonicWALL GAV can be configured to protect against internal threats as well as those originating outside the network. It operates over a multitude of protocols including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols, to provide administrators with comprehensive network threat prevention and control. Because files containing malicious code and viruses can also be compressed and therefore inaccessible to conventional anti-virus solutions, SonicWALL GAV integrates advanced decompression technology that automatically decompresses and scans files on a per packet basis.

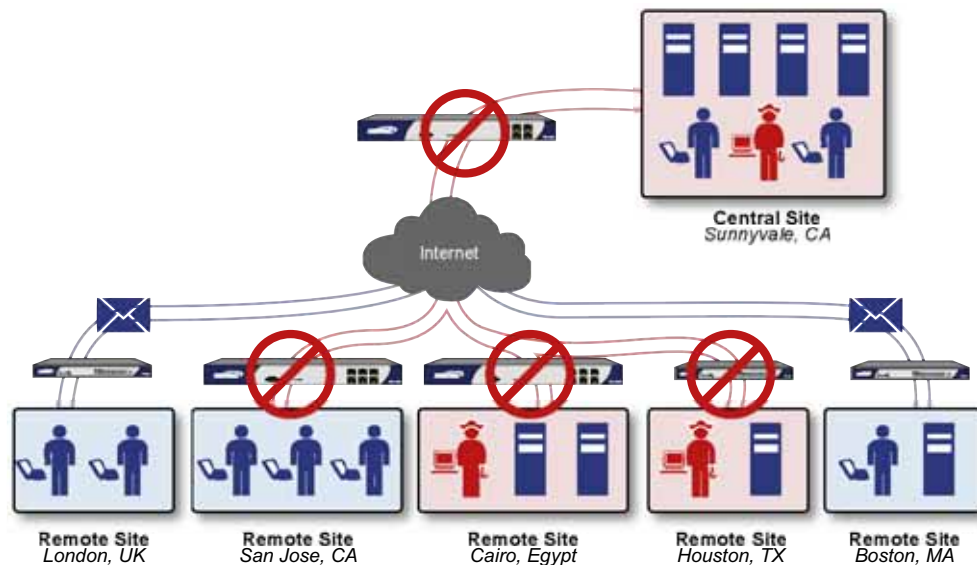
## SonicWALL GAV Multi-Layered Approach

SonicWALL GAV delivers comprehensive, multi-layered anti-virus protection for networks at the desktop, the network, and at remote sites. SonicWALL GAV enforces anti-virus policies at the gateway to ensure all users have the latest updates and monitors files as they come into the network.



## Remote Site Protection

- Step 1** Users send typical e-mail and files between remote sites and the corporate office.
- Step 2** SonicWALL GAV scans and analyses files and e-mail messages on the SonicWALL security appliance.
- Step 3** Viruses are found and blocked before infecting remote desktop.
- Step 4** Virus is logged and alert is sent to administrator.



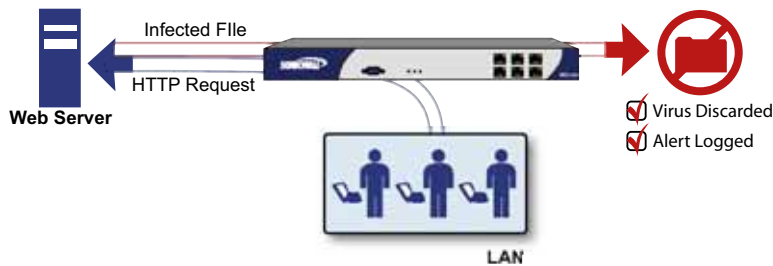
## Internal Network Protection

- Step 1** Internal user contracts a virus and releases it internally.
- Step 2** All files are scanned at the gateway before being received by other network users.
- Step 3** If virus is found, file is discarded.
- Step 4** Virus is logged and alert is sent to administrator.



## HTTP File Downloads

- Step 1** Client makes a request to download a file from the Web.
- Step 2** File is downloaded through the Internet.
- Step 3** File is analyzed the SonicWALL GAV engine for malicious code and viruses.
- Step 4** If virus found, file discarded.
- Step 5** Virus is logged and alert sent to administrator.



## Server Protection

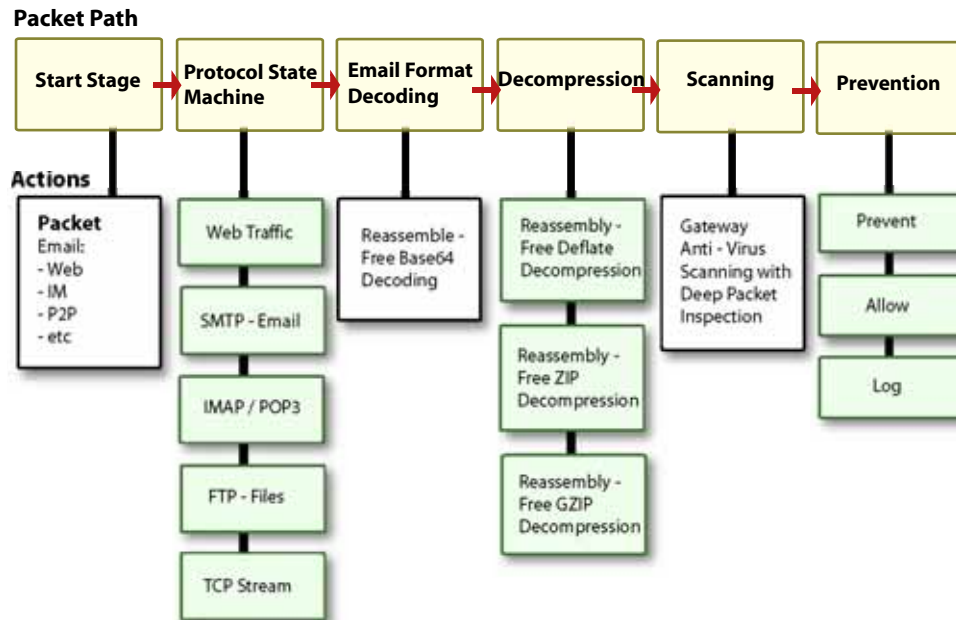
- Step 1** Outside user sends an incoming e-mail.
- Step 2** E-mail is analyzed the SonicWALL GAV engine for malicious code and viruses before received by e-mail server.
- Step 3** If virus found, threat prevented.
- Step 4** E-mail is returned to sender, virus is logged, and alert sent to administrator.



## SonicWALL GAV Architecture

SonicWALL GAV is based on SonicWALL's high performance DPIv2.0 engine (Deep Packet Inspection version 2.0) engine, which performs all scanning directly on the SonicWALL security appliance. SonicWALL GAV includes advanced decompression technology that can automatically decompress and scan files on a per packet basis to search for viruses and malware. The SonicWALL GAV engine can perform base64 decoding without ever reassembling the entire base64 encoded mail stream. Because SonicWALL's GAV does not have to perform reassembly, there are no file-size limitations imposed by the scanning engine. Base64 decoding and ZIP, LHZ, and GZIP (LZ77) decompression are also performed on a

single-pass, per-packet basis. Reassembly free virus scanning functionality of the SonicWALL GAV engine is inherited from the Deep Packet Inspection engine, which is capable of scanning streams without ever buffering any of the bytes within the stream.



Building on SonicWALL's reassembly-free architecture, GAV has the ability to inspect multiple application protocols, as well as generic TCP streams, and compressed traffic. SonicWALL GAV protocol inspection is based on high performance state machines which are specific to each supported protocol. SonicWALL GAV delivers protection by inspecting over the most common protocols used in today's networked environments, including SMTP, POP3, IMAP, HTTP, FTP, NetBIOS, instant messaging and peer-to-peer applications and dozens of other stream-based protocols. This closes potential backdoors that can be used to compromise the network while also improving employee productivity and conserving Internet bandwidth.



#### Tip

If your SonicWALL security appliance is connected to the Internet and registered at [mySonicWALL.com](http://mySonicWALL.com), you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Virus, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.



#### Note

Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL documentation Web site: <http://www.sonicwall.com/us/Support.html>

## Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL security appliance management interface.



**Note** If you already have a mysonicWALL.com account, go to [“Registering Your SonicWALL Security Appliance”](#) on page 721.

- Step 1** Log into the SonicWALL security appliance management interface.
- Step 2** If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



- Step 4** In the mySonicWALL.com Login page, click the [here](#) link in **If you do not have a mySonicWALL account, please click here to create one.**



- Step 5** In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields.



**Note** Remember your username and password to access your mySonicWALL.com account.

- Step 6** Click **Submit** after completing the **MySonicWALL Account** form.
- Step 7** When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.
- Congratulations.** Your mySonicWALL.com account is activated.
- Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.



**Note** mySonicWALL.com registration information is not sold or shared with any other company.



## Registering Your SonicWALL Security Appliance

- 
- Step 1** Log into the SonicWALL security appliance management interface.
- Step 2** If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.
- Step 4** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
- Step 5** The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
- **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
  - **Client Anti-Virus** - Provides desktop and server anti-virus protection with software running on each computer.
  - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
  - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
  - **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.
- Click **Continue** on each page.




---

**Note** Clicking on the **Continue** button does not activate the FREE TRIAL versions of these SonicWALL Security Services.

---

- Step 6** At the top of the **Product Survey** page, Enter a “friendly name” for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
- Step 7** Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
- Step 8** Click **Submit**.
- Step 9** When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

## Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Because SonicWALL Anti-Spyware is part of SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- Step 1** On the **Security Services > Gateway Anti-Virus** page, click the **SonicWALL Gateway Anti-Virus Subscription** link. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- Step 4** Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Anti-Virus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Free Trial		Renew		07 Apr 2005
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

You can apply the following activation keys:  
 ANTI SPYWARE 1 YR BUNDLE ASMUYZF8  
 SNWL GAV 1 YR BUNDLE (PS/GAV BUNDLE) GAMUYZF8

- Step 5** Click on the Anti-Spyware link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 6** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.
- Step 7** Click on the SonicWALL Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 8** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on mySonicWALL.com, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

## Activating FREE TRIALS

You can try FREE TRIAL versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

- 
- Step 1** Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
  - Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
  - Step 3** Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

## Setting Up SonicWALL Gateway Anti-Virus Protection

Activating the SonicWALL Gateway Anti-Virus license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Gateway Anti-Virus to begin protecting your network, you need to perform the following steps:

- 
- Step 1** Enable SonicWALL Gateway Anti-Virus.
  - Step 2** Apply SonicWALL Gateway Anti-Virus Protection to Zones.

**Note**

For complete instructions on setting up SonicWALL Gateway Anti-Virus, refer to the [SonicWALL Gateway Anti-Virus Administrator's Guide](#) available on the SonicWALL documentation Web site: <http://www.sonicwall.com/us/Support.html>.

---

The **Security Services > Gateway Anti-Virus** page provides the settings for configuring SonicWALL GAV on your SonicWALL security appliance.

## Enabling SonicWALL GAV

You must select **Enable Gateway Anti-Virus** check box in the **Gateway Anti-Virus Global Settings** section to enable SonicWALL GAV on your SonicWALL security appliance. You must specify the Zones you want SonicWALL GAV protection on the **Network > Zones** page.

## Applying SonicWALL GAV Protection on Interfaces

You apply SonicWALL GAV to Zones on the **Network > Zones** page.



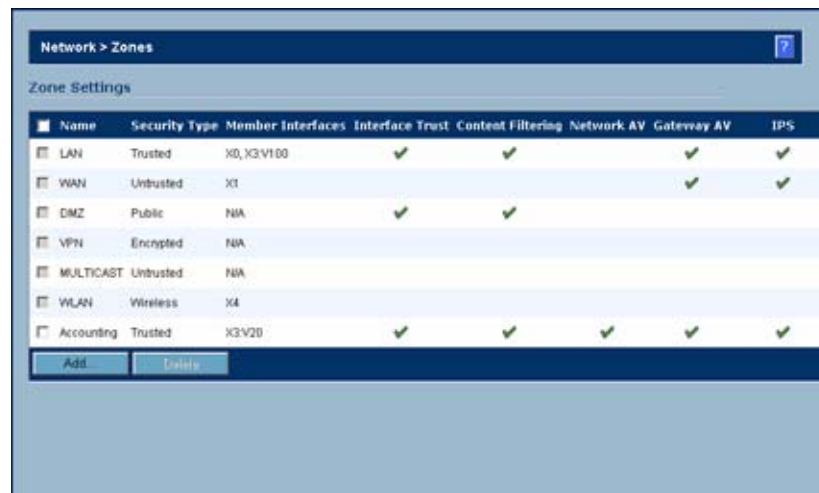
### Note

Refer to [“Applying SonicWALL GAV Protection on Zones” on page 725](#) for instructions on applying SonicWALL GAV protection to zones.

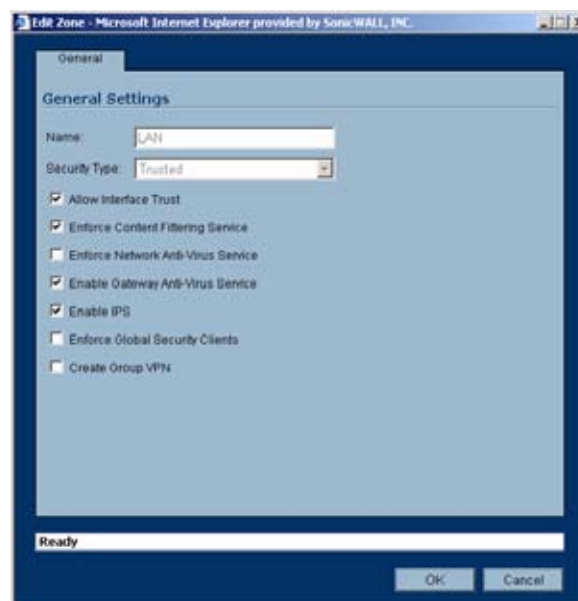
## Applying SonicWALL GAV Protection on Zones

You can enforce SonicWALL GAV not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL GAV on the LAN zone enforces anti-virus protection on all incoming and outgoing LAN traffic.

- Step 1** In the SonicWALL security appliance management interface, select **Network > Zones** or from the **Gateway Anti-Virus Status** section, on the **Security Services > Gateway Anti-Virus** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.



- Step 2** In the **Configure** column in the **Zone Settings** table, click the edit icon . The **Edit Zone** window is displayed.



- Step 3** Click the **Enable Gateway Anti-Virus Service** checkbox. A checkmark appears. To disable Gateway Anti-Virus Service, uncheck the box.

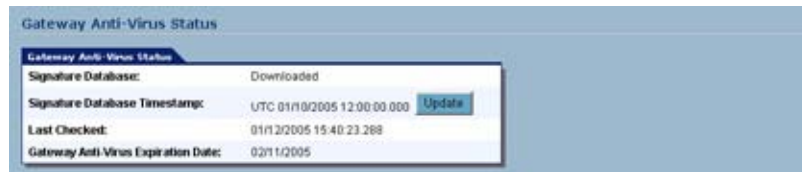
- Step 4** Click **OK**.

**Note**

You also enable SonicWALL GAV protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.

## Viewing SonicWALL GAV Status Information

The **Gateway Anti-Virus Status** section shows the state of the anti-virus signature database, including the database's timestamp, and the time the SonicWALL signature servers were last checked for the most current database version. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.



The **Gateway Anti-Virus Status** section displays the following information:

- **Signature Database** indicates whether the signature database needs to be downloaded or has been downloaded.
- **Signature Database Timestamp** displays the last update to the SonicWALL GAV signature database, not the last update to your SonicWALL security appliance.
- **Last Checked** indicates the last time the SonicWALL security appliance checked the signature database for updates. The SonicWALL security appliance automatically attempts to synchronize the database on startup, and once every hour.
- **Gateway Anti-Virus Expiration Date** indicates the date when the SonicWALL GAV service expires. If your SonicWALL GAV subscription expires, the SonicWALL IPS inspection is stopped and the SonicWALL GAV configuration settings are removed from the SonicWALL security appliance. These settings are automatically restored after renewing your SonicWALL GAV license to the previously configured state.

The **Gateway Anti-Virus Status** section displays **Note: Enable the Gateway Anti-Virus per zone from the [Network > Zones](#) page**. Clicking on the **Network > Zones** link displays the **Network > Zones** page for applying SonicWALL GAV on Zones.

**Note**

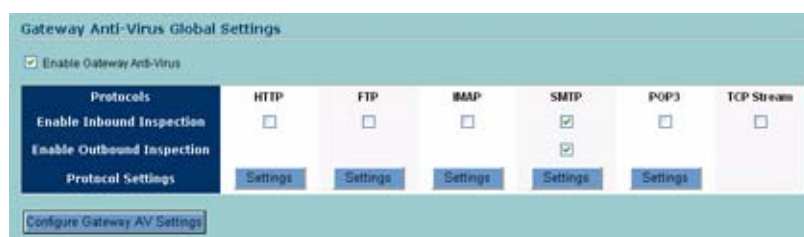
Refer to [“Applying SonicWALL GAV Protection on Zones” on page 725](#) for instructions on applying SonicWALL GAV protection to zones.

## Updating SonicWALL GAV Signatures

By default, the SonicWALL security appliance running SonicWALL GAV automatically checks the SonicWALL signature servers once an hour. There is no need for an administrator to constantly check for new signature updates. You can also manually update your SonicWALL GAV database at any time by clicking the **Update** button located in the **Gateway Anti-Virus Status** section.

SonicWALL GAV signature updates are secured. The SonicWALL security appliance must first authenticate itself with a pre-shared secret, created during the SonicWALL Distributed Enforcement Architecture licensing registration. The signature request is transported through HTTPS, along with full server certificate verification.

## Specifying Protocol Filtering



Application-level awareness of the type of protocol that is transporting the violation allows SonicWALL GAV to perform specific actions within the context of the application to gracefully handle the rejection of the payload.

By default, SonicWALL GAV inspects all inbound **HTTP**, **FTP**, **IMAP**, **SMTP** and **POP3** traffic. Generic **TCP Stream** can optionally be enabled to inspect all other TCP based traffic, such as non-standard ports of operation for SMTP and POP3, and IM and P2P protocols.

## Enabling Inbound Inspection

Within the context of SonicWALL GAV, the **Enable Inbound Inspection** protocol traffic handling refers to the following:

- Non-SMTP traffic initiating from a Trusted, Wireless, or Encrypted Zone destined to any Zone.
- Non-SMTP traffic from a Public Zone destined to an Untrusted Zone.
- SMTP traffic initiating from a non-Trusted Zone destined to a Trusted, Wireless, Encrypted, or Public Zone.
- SMTP traffic initiating from a Trusted, Wireless, or Encrypted Zone destined to a Trusted, Wireless, or Encrypted Zone.

The **Enable Inbound Inspection** protocol traffic handling represented as a table:

SMTP Traffic					
From \ To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✗	✗
Encrypted	✓	✓	✓	✗	✗
Wireless	✓	✓	✓	✗	✗
Public	✓	✓	✓	✓	✓
Untrusted	✓	✓	✓	✓	✓

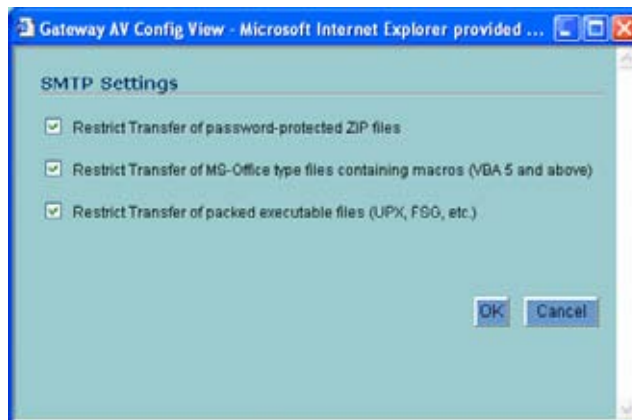
All Other Traffic					
From \ To	Trusted	Encrypted	Wireless	Public	Untrusted
Trusted	✓	✓	✓	✓	✓
Encrypted	✓	✓	✓	✓	✓
Wireless	✓	✓	✓	✓	✓
Public	✗	✗	✗	✗	✓
Untrusted	✗	✗	✗	✗	✗

## Enabling Outbound SMTP Inspection

The **Enable Outbound Inspection** feature is available for SMTP traffic, such as for a mail server that might be hosted on the DMZ. Enabling outbound inspection for SMTP scans mail that is delivered to the internally hosted SMTP server for viruses.

## Restricting File Transfers

For each protocol you can restrict the transfer of files with specific attributes by clicking on the **Settings** button under the protocol in the **Gateway Anti-Virus Global Settings** section.



These restrict transfer settings include:



- **Restrict Transfer of password-protected Zip files** - Disables the transfer of password protected ZIP files over any enabled protocol. This option only functions on protocols (e.g. HTTP, FTP, SMTP) that are enabled for inspection.
- **Restrict Transfer of MS-Office type files containing macros (VBA 5 and above)** - Disables the transfers of any MS Office 97 and above files that contain VBA macros.
- **Restrict Transfer of packed executable files (UPX, FSG, etc.)** - Disables the transfer of packed executable files. Packers are utilities which compress and sometimes encrypt executables. Although there are legitimate applications for these, they are also sometimes used with the intent of obfuscation, so as to make the executables less detectable by anti-virus applications. The packer adds a header that expands the file in memory, and then executes that file. SonicWALL Gateway Anti-Virus currently recognizes the most common packed formats: UPX, FSG, PKLite32, Petite, and ASPack. additional formats are dynamically added along with SonicWALL GAV signature updates.

## Configuring Gateway AV Settings

Clicking the **Configure Gateway AV Settings** button at the bottom of the **Gateway Anti-Virus Global Settings** section displays the **Gateway AV Settings** window, which allows you to configure clientless notification alerts and create a SonicWALL GAV exclusion list.

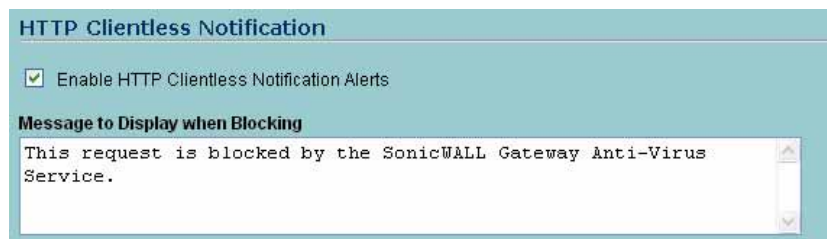




If you want to suppress the sending of e-mail messages (SMTP) to clients from SonicWALL GAV when a virus is detected in an e-mail or attachment, check the **Disable SMTP Responses** box.

## Configuring HTTP Clientless Notification

The HTTP Clientless Notification feature notifies users when GAV detects an incoming threat from an HTTP server. To configure this feature, check the Enable HTTP Clientless Notification Alerts box and enter a message in the Message to Display when Blocking field, as shown below.



With this option disabled, when GAV detects an incoming threat from an HTTP server, GAV blocks the threat and the user receives a blank HTTP page. Typically, users will attempt to reload the page because they are not aware of the threat. The HTTP Clientless Notification feature informs the user that GAV detected a threat from the HTTP server.



**Tip**

The HTTP Clientless Notification feature is also available for SonicWALL Anti-Spyware.

Optionally, you can configure the timeout for the HTTP Clientless Notification on the **Security Services > Summary** page under the **Security Services Summary** heading.

## Configuring a SonicWALL GAV Exclusion List

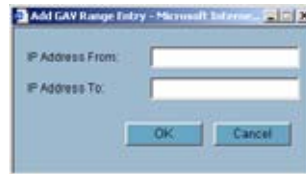
Any IP addresses listed in the exclusion list bypass virus scanning on their traffic. The **Gateway AV Exclusion List** section provides the ability to define a range of IP addresses whose traffic will be excluded from SonicWALL GAV scanning.



**Warning** Use caution when specifying exclusions to SonicWALL GAV protection.

To add an IP address range for exclusion, perform these steps:

- Step 1** Click the **Enable Gateway AV Exclusion List** checkbox to enable the exclusion list.
- Step 2** Click the **Add** button. The **Add GAV Range Entry** window is displayed.



- Step 3** Enter the IP address range in the **IP Address From** and **IP Address To** fields, then click **OK**. Your IP address range appears in the **Gateway AV Exclusion List** table. Click the edit icon in the **Configure** column to change an entry or click the trashcan icon to delete an entry.
- Step 4** Click **OK** to exit the **Gateway AV Config View** window.

## Viewing SonicWALL GAV Signatures

The **Gateway Anti-Virus Signatures** section allows you to view the contents of the SonicWALL GAV signature database. All the entries displayed in the **Gateway Anti-Virus Signatures** table are from the SonicWALL GAV signature database downloaded to your SonicWALL security appliance.

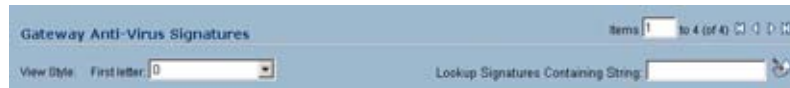


#	Name
1	0.0 (VOEN)
2	0190 (Dialer)
3	0190-dialer.com (Dialer)
4	0190-dialer.com 2 (Dialer)
5	1 (3tone)
6	1005.0 (VOEN)
7	102 (BAT.MF)
8	116 (BAT.MF)
9	1168.512 (VOEN)
10	1168.512 (VOEN)
11	117.0 (VOEN)
12	1178.512 (VOEN)
13	118.32 (VOEN)
14	119.256 (VOEN)
15	1193.3 (VOEN)
16	12001.726 (VOEN)
17	12049.512 (VOEN)



**Note** Signature entries in the database change over time in response to new threats.

## Displaying Signatures



You can display the signatures in a variety of views using the **View Style** menu.

- **Use Search String** - Allows you to display signatures containing a specified string entered in the Lookup Signatures **Containing String** field.
- **All Signatures** - Displays all the signatures in the table, 50 to a page.
- **0 - 9** - Displays signature names beginning with the number you select from the menu.
- **A-Z** - Displays signature names beginning with the letter you select from menu.

## Navigating the Gateway Anti-Virus Signatures Table

The SonicWALL GAV signatures are displayed fifty to a page in the **Gateway Anti-Virus Signatures** table. The **Items** field displays the table number of the first signature. If you're displaying the first page of a signature table, the entry might be **Items 1 to 50 (of 58)**. Use the navigation buttons to navigate the table.



## Searching the Gateway Anti-Virus Signature Database

You can search the signature database by entering a search string in the **Lookup Signatures Containing String** field, then clicking the edit (Notepad) icon.

Lookup Signatures Containing String:  

The signatures that match the specified string are displayed in the **Gateway Anti-Virus Signatures** table.





## CHAPTER 58

# Activating Intrusion Prevention Service

---

## Security Services > Intrusion Prevention Service

SonicWALL Intrusion Prevention Service (SonicWALL IPS) delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS. SonicWALL IPS is designed to protect against application vulnerabilities as well as worms, Trojans, and peer-to-peer, spyware and backdoor exploits. The extensible signature language used in SonicWALL's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. SonicWALL IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new hacker attacks through SonicWALL's industry-leading Distributed Enforcement Architecture (DEA). Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.

### SonicWALL Deep Packet Inspection

Deep Packet Inspection looks at the data portion of the packet. The Deep Packet Inspection technology includes intrusion detection and intrusion prevention. Intrusion detection finds anomalies in the traffic and alerts the administrator. Intrusion prevention finds the anomalies in the traffic and reacts to it, preventing the traffic from passing through.

Deep Packet Inspection is a technology that allows a SonicWALL Security Appliance to classify passing traffic based on rules. These rules include information about layer 3 and layer 4 content of the packet as well as the information that describes the contents of the packet's payload, including the application data (for example, an FTP session, an HTTP Web browser session, or even a middleware database connection). This technology allows the administrator to detect and log intrusions that pass through the SonicWALL Security Appliance, as well as prevent them (i.e. dropping the packet or resetting the TCP connection). SonicWALL's Deep Packet Inspection technology also correctly handles TCP fragmented byte stream inspection as if no TCP fragmentation has occurred.

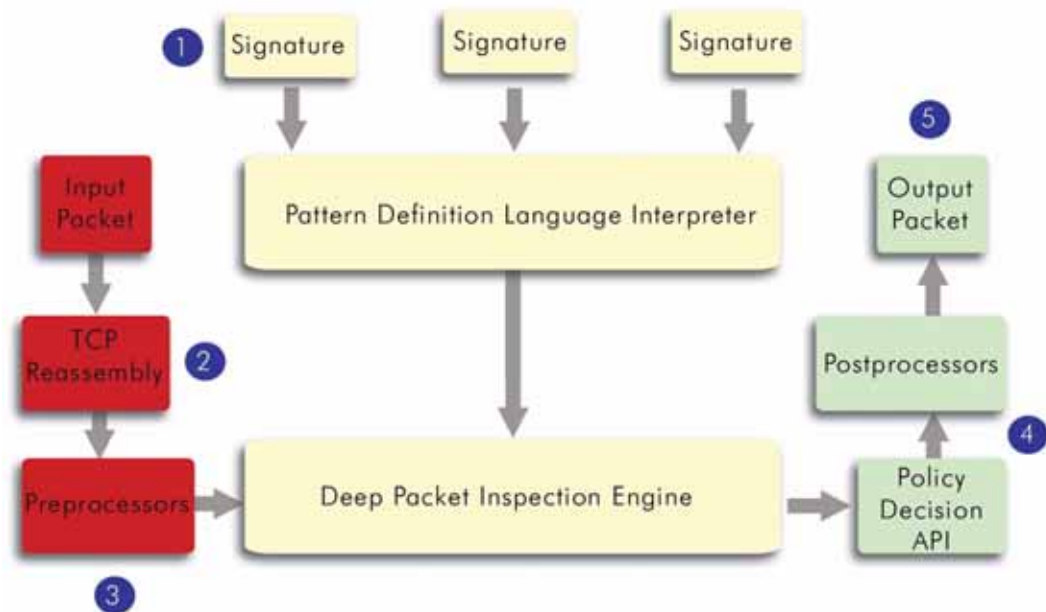
## How SonicWALL's Deep Packet Inspection Works

Deep Packet Inspection technology enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities. This is the technology behind SonicWALL Intrusion Prevention Service. SonicWALL's Deep Packet Inspection technology enables dynamic signature updates pushed from the SonicWALL Distributed Enforcement Architecture.

The following steps describe how the SonicWALL Deep Packet Inspection Architecture works:

- Step 1** Pattern Definition Language Interpreter uses signatures that can be written to detect and prevent against known and unknown protocols, applications and exploits.
- Step 2** TCP packets arriving out-of-order are reassembled by the Deep Packet Inspection framework.
- Step 3** Deep Packet Inspection engine preprocessing involves normalization of the packet's payload. For example, a HTTP request may be URL encoded and thus the request is URL decoded in order to perform correct pattern matching on the payload.
- Step 4** Deep Packet Inspection engine postprocessors perform actions which may either simply pass the packet without modification, or could drop a packet or could even reset a TCP connection.
- Step 5** SonicWALL's Deep Packet Inspection framework supports complete signature matching across the TCP fragments without performing any reassembly (unless the packets are out of order). This results in more efficient use of processor and memory for greater performance.

### SonicWALL DEEP PACKET INSPECTION ARCHITECTURE



## SonicWALL IPS Terminology

- **Stateful Packet Inspection** - looking at the header of the packet to control access based on port, protocol, and IP address.



- **Deep Packet Inspection** - looking at the data portion of the packet. Enables the firewall to investigate farther into the protocol to examine information at the application layer and defend against attacks targeting application vulnerabilities.
- **Intrusion Detection** - a process of identifying and flagging malicious activity aimed at information technology.
- **False Positive** - a falsely identified attack traffic pattern.
- **Intrusion Prevention** - finding anomalies and malicious activity in traffic and reacting to it.
- **Snort** - an open source network intrusion detection system. SonicWALL IPS includes open-source Snort signatures, as well as signatures from other signature databases, and SonicWALL created signatures. SonicWALL does not use the Snort engine.
- **Signature** - code written to detect and prevent intrusions, worms, application exploits, and Peer-to-Peer and Instant Messaging traffic.

## SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface.

Because SonicWALL Intrusion Prevention Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need the following:

- **SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).
- **mySonicWALL.com account.** Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form from your SonicWALL security appliance management interface. Your mySonicWALL.com account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser.
- **Registered SonicWALL security appliance with active Internet connection.** Registering your SonicWALL security appliance is a simple procedure done directly from the management interface.
- **SonicOS Enhanced 3.1 or newer.** Your SonicWALL security appliance must be running SonicOS Enhanced 3.1 or newer for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

**Tip**

If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

**Note**

Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL documentation Web site: <http://www.sonicwall.com/us/Support.html>

## Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL security appliance management interface.

**Note**

If you already have a mysonicWALL.com account, go to “[Registering Your SonicWALL Security Appliance](#)” on page 739.

- Step 1** Log into the SonicWALL security appliance management interface.
- Step 2** If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



- Step 4** In the mySonicWALL.com Login page, click the [here](#) link in **If you do not have a mySonicWALL account, please click here to create one.**



- Step 5** In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields.



**Note** Remember your username and password to access your mySonicWALL.com account.

**Step 6** Click **Submit** after completing the **MySonicWALL Account** form.

**Step 7** When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue. Congratulations.** Your mySonicWALL.com account is activated. Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.



**Note** mySonicWALL.com registration information is not sold or shared with any other company.

## Registering Your SonicWALL Security Appliance

To register your SonicWALL Security Appliance, perform the following steps:

- 
- Step 1** Log into the SonicWALL security appliance management interface.
- Step 2** If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.
- Step 4** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
- Step 5** The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
- **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
  - **Client Anti-Virus** - Provides desktop and server anti-virus protection with software running on each computer.
  - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
  - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
  - **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.

Click **Continue** on each page.



**Note** Clicking on the **Continue** button does not activate the FREE TRIAL versions of these SonicWALL Security Services.

- Step 6** At the top of the **Product Survey** page, Enter a “friendly name” for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
- Step 7** Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
- Step 8** Click **Submit**.
- Step 9** When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

## Activating FREE TRIALS

You can try FREE TRIAL versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

- Step 1** Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
- Step 3** Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

## Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Because SonicWALL Intrusion Prevention Service is part of SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- Step 1** On the **Security Services > Intrusion Prevention** page, click the **SonicWALL Intrusion Prevention Service Subscription** link. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- Step 4** Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

Security Service	States	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade, Renew, Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway AntiVirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Free Trial		Renew		07 Apr 2005
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

You can apply the following activation keys:

ANTI SPYWARE 1 YR BUNDLE ASMUJZF8  
 SNWL GAV 1 YR BUNDLE (IPS/GAV BUNDLE) GAMUJZF8

- Step 5** Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 6** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.
- Step 7** Click on the SonicWALL Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 8** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on mySonicWALL.com, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

## Setting Up SonicWALL Intrusion Prevention Service Protection

Activating the SonicWALL Intrusion Prevention Service license on your SonicWALL security appliance does not automatically enable the protection. To configure SonicWALL Intrusion Prevention Service to begin protecting your network, you need to perform the following steps:

- 
- Step 1** Enable SonicWALL Intrusion Prevention Service.
  - Step 2** Specify the Priority attack Groups.
  - Step 3** Apply SonicWALL Intrusion Prevention Service Protection to Zones.



### Note

For complete instructions on setting up SonicWALL Intrusion Prevention Service, refer to the [SonicWALL Intrusion Prevention Service Administrator's Guide](http://www.sonicwall.com/us/Support.html) available on the SonicWALL documentation Web site <http://www.sonicwall.com/us/Support.html>.

Selecting **Security Services > Intrusion Prevention** displays the configuration settings for SonicWALL IPS on your SonicWALL security appliance.

The **Intrusion Prevention Service** page is divided into three sections:

- **IPS Status** - displays status information on the state of the signature database, your SonicWALL IPS license, and other information.
- **IPS Global Settings** - provides the key settings for enabling SonicWALL IPS on your SonicWALL security appliance, specifying global SonicWALL IPS protection based on three classes of attacks, and other configuration options.
- **IPS Policies** - allows you to view SonicWALL IPS signatures and configure the handling of signatures by category groups or on a signature by signature basis. Categories are signatures grouped together based on the type of attack.

After activating your Intrusion Prevention Service license, you must enable and configure SonicWALL IPS on the SonicWALL management interface to before intrusion prevention policies are applied to your network traffic.

## Enabling SonicWALL IPS

SonicWALL IPS must be globally enabled on your SonicWALL security appliance by checking the **Enable IPS** check box in the **IPS Global Settings** section. A checkmark in the **Enable IPS** check box turns on the service on your SonicWALL security appliance.



### Note

Checking the **Enable IPS** check box does not automatically start SonicWALL IPS protection. You must also in the **IPS Global Settings** section. You must specify a **Prevent All** action in the **Signature Groups** table to activate intrusion prevention on the SonicWALL security appliance, and specify the interface or zones you want to protect.

## Specifying Global Attack Level Protection

SonicWALL IPS allows you to globally manage your network protection against attacks by simply selecting the class of attacks: **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks**. Selecting the **Prevent All** and **Detect All** check boxes for **High Priority Attacks** and **Medium Priority Attacks** in the **Signature Groups** table, and then clicking **Apply** protects your network against the most dangerous and disruptive attacks. For more detailed

information on configuring global signature groups, refer to “Configuring Global Signature Groups” in the *SonicWALL Intrusion Prevention Service Administrator’s Guide* available on the SonicWALL Resource CD or at [www.sonicwall.com/support/documentation.html](http://www.sonicwall.com/support/documentation.html)

**Note**


Leaving the **High Priority Attacks**, **Medium Priority Attacks**, and **Low Priority Attacks** signature groups with no **Prevent All** action checked means no intrusion prevention is occurring on the SonicWALL security appliance.

## Applying SonicWALL IPS Protection on Zones

You apply SonicWALL IPS to Zones on the **Network > Zones** page to enforce SonicWALL IPS not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL IPS on the LAN zone enforces SonicWALL IPS on all incoming and outgoing LAN traffic.

In the **IPS Status** section of the **Security Services > Intrusion Prevention Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply SonicWALL IPS to a zone listed on the **Network > Zones** page.

To enable SonicWALL on a zone, perform these steps:

- 
- Step 1** In the SonicWALL security appliance management interface, select **Network > Zones** or from the **IPS Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link. The **Network > Zones** page is displayed.
  - Step 2** In the **Configure** column in the **Zone Settings** table, click the edit icon  for the zone you want to apply SonicWALL IPS. The **Edit Zone** window is displayed.
  - Step 3** Click the **Enable IPS** checkbox. A checkmark appears. To disable SonicWALL IPS, uncheck the box.
  - Step 4** Click **OK**.

You also enable SonicWALL IPS protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.







## CHAPTER 59

# Activating Anti-Spyware Service

---

## Security Services > Anti-Spyware Service

SonicWALL Anti-Spyware is part of the SonicWALL Gateway Anti-Virus, Anti-Virus and Intrusion Prevention Service solution that provides comprehensive, real-time protection against viruses, worms, Trojans, spyware, and software vulnerabilities.

The SonicWALL Anti-Spyware Service protects networks from intrusive spyware by cutting off spyware installations and delivery at the gateway and denying previously installed spyware from communicating collected information outbound. SonicWALL Anti-Spyware works with other anti-spyware program, such as programs that remove existing spyware applications from hosts. You are encouraged to use or install host-based anti-spyware software as an added measure of defense against spyware.

SonicWALL Anti-Spyware analyzes inbound connections for the most common method of spyware delivery, ActiveX-based component installations. It also examines inbound setup executables and cabinet files crossing the gateway, and resets the connections that are streaming spyware setup files to the LAN. These file packages may be freeware bundled with adware, keyloggers, or other spyware. If spyware has been installed on a LAN workstation prior to the SonicWALL Anti-Spyware solution install, the service will examine outbound traffic for streams originating at spyware infected clients and reset those connections. For example, when spyware has been profiling a user's browsing habits and attempts to send the profile information home, the SonicWALL security appliance identifies that traffic and resets the connection.

The SonicWALL Anti-Spyware Service provides the following protection:

- Blocks spyware delivered through auto-installed ActiveX components, the most common vehicle for distributing malicious spyware programs.
- Scans and logs spyware threats that are transmitted through the network and alerts administrators when new spyware is detected and/or blocked.
- Stops existing spyware programs from communicating in the background with hackers and servers on the Internet, preventing the transfer of confidential information.
- Provides granular control over networked applications by enabling administrators to selectively permit or deny the installation of spyware programs.
- Prevents e-mailed spyware threats by scanning and then blocking infected e-mails transmitted either through SMTP, IMAP or Web-based e-mail.

**Note**

Refer to the SonicWALL Anti-Spyware Administrator's Guide on the SonicWALL Web site: <http://www.sonicwall.com/us/Support.html> for complete product documentation. SonicWALL Deep Packet Inspection

## SonicWALL Gateway Anti-Virus, Anti-Spyware, and IPS Activation

If you do not have SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service installed on your SonicWALL security appliance, the **Security Services > Anti-Spyware** page indicates an upgrade is required and includes a link to activate it from your SonicWALL security appliance management interface.

Because SonicWALL Intrusion Prevention Service is part of the unified SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, you will have a single License Key to activate all three services on your SonicWALL security appliance.

You must activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from the **Security Services > Intrusion Prevention** page first. Once you have activated Intrusion Prevention Service, you can then activate SonicWALL Gateway Anti-Virus and SonicWALL Anti-Spyware.

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service on your SonicWALL security appliance, you need the following:

- **SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license.** You need to purchase a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service license from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).
- **mySonicWALL.com account.** Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form from your SonicWALL security appliance management interface. Your mySonicWALL.com account is also accessible at <https://www.mysonicwall.com> from any Internet connection with a Web browser.
- **Registered SonicWALL security appliance with active Internet connection.** Registering your SonicWALL security appliance is a simple procedure done directly from the management interface.
- **SonicOS Enhanced 3.1 or newer.** Your SonicWALL security appliance must be running SonicOS Enhanced 3.1 or newer for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

**Tip**

If your SonicWALL security appliance is connected to the Internet and registered at mySonicWALL.com, you can activate a 30-day FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service separately from the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, and **Security Services > Intrusion Prevention** pages in the management interface.

**Note**

Administrator Guides for SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service are available on the SonicWALL documentation Web site: <http://www.sonicwall.com/us/Support.html>

## Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL security appliance management interface.



**Note** If you already have a mysonicWALL.com account, go to [“Registering Your SonicWALL Security Appliance”](#) on page 748.

- Step 1** Log into the SonicWALL security appliance management interface.
- Step 2** If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



- Step 4** In the **mySonicWALL.com Login** page, click the **here** link in **If you do not have a mySonicWALL account, please click here to create one.**



- Step 5** In the **MySonicWall Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields.



**Note** Remember your username and password to access your mySonicWALL.com account.

- Step 6** Click **Submit** after completing the **MySonicWALL Account** form.
- Step 7** When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**.

**Congratulations.** Your mySonicWALL.com account is activated.

Now you need to log into mySonicWALL.com to register your SonicWALL security appliance.



**Note** mySonicWALL.com registration information is not sold or shared with any other company.

## Registering Your SonicWALL Security Appliance

- 
- Step 1** Log into the SonicWALL security appliance management interface.
- Step 2** If the **System > Status** page is not displaying in the management interface, click **System** in the left-navigation menu, and then click **Status**.
- Step 3** On the **System > Status** page, in the **Security Services** section, click the **Register** link. The **mySonicWALL.com Login** page is displayed.
- Step 4** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
- Step 5** The next several pages inform you about the free trials available to you for SonicWALL's Security Services:
- **Gateway Anti-Virus** - Delivers real-time virus protection for your entire network.
  - **Client Anti-Virus** - Provides desktop and server anti-virus protection with software running on each computer.
  - **Premium Content Filtering Service** - Enhances productivity by limiting access to objectionable Web content.
  - **Intrusion Prevention Service** - Protects your network against worms, Trojans, and application layer attacks.
  - **Anti-Spyware** - Protects your network from malicious spyware by blocking spyware installations at the gateway and disrupts.

Click **Continue** on each page.



**Note** Clicking on the **Continue** button does not activate the FREE TRIAL versions of these SonicWALL Security Services.

- 
- Step 6** At the top of the **Product Survey** page, Enter a "friendly name" for your SonicWALL content security appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
- Step 7** Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
- Step 8** Click **Submit**.
- Step 9** When the mySonicWALL.com server has finished processing your registration, a page is displayed informing you that the SonicWALL security appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you the available services. You can activate the service from this page or the specific service page under the **Security Services** left-navigation menu in the management interface.

## Activating FREE TRIALS

You can try FREE TRIAL versions of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, and SonicWALL Intrusion Prevention Service. You must activate each service separately from the Manage Services Online table on the **System > Licenses** page or by clicking the FREE TRIAL link on the respective Security Services page (i.e. **Security Services > Gateway Anti-Virus**).

To try a FREE TRIAL of SonicWALL Gateway Anti-Virus, SonicWALL Anti-Spyware, or SonicWALL Intrusion Prevention Service, perform these steps:

- 
- Step 1** Click the **FREE TRIAL** link on the **Security Services > Gateway Anti-Virus**, **Security Services > Anti-Spyware**, or **Security Services > Intrusion Prevention** page. The **mySonicWALL.com Login** page is displayed.
  - Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **FREE TRIAL** link.
  - Step 3** Click **Try** in the **FREE TRIAL** column in the **Manage Services Online** table. The service is enabled on your security appliance.

## Activating the Gateway Anti-Virus, Anti-Spyware, and IPS License

Because SonicWALL Intrusion Prevention Service is part of SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. The Activation Key you receive is for all three services on your SonicWALL security appliance.

If you do not have a SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service. license activated on your SonicWALL security appliance, you must purchase it from a SonicWALL reseller or through your mySonicWALL.com account (limited to customers in the USA and Canada).

If you have an Activation Key for SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service, perform these steps to activate the combined services:

- Step 1** On the **Security Services > Intrusion Prevention** page, click the **SonicWALL Intrusion Prevention Service Subscription** link. The **mySonicWALL.com Login** page is displayed.
- Step 2** Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. If your SonicWALL security appliance is already registered to your mySonicWALL.com account, the **System > Licenses** page appears.
- Step 3** Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table.
- Step 4** Type in the Activation Key in the **New License Key** field and click **Submit**. SonicWALL Intrusion Prevention Service is activated. The **System > Licenses** page is displayed with the Anti-Spyware and Gateway Anti-Virus links displayed at the bottom of the **Manage Services Online** table with the child Activation Keys.

Security Service	Status	Free Trial	Manage Service	Count	Expiration
Nodes/Users	Licensed			Unlimited	
Network Anti-Virus	Expired		Upgrade Renew Share	5	21 Feb 2004
Intrusion Prevention Service	Licensed		Renew		09 Mar 2006
SonicAV	Not Licensed	Try	Activate		
Gateway Antivirus	Not Licensed	Try	Activate		
Server Anti-Virus	Not Licensed		Activate		
Anti-Spyware	Free Trial		Renew		07 Apr 2005
CFS Standard	Expired		Renew		21 Feb 2004
CFS Premium Service	Expired		Renew		26 Aug 2004
E-Mail Filtering Service	Licensed				
VPN	Licensed				
Global VPN Client	Licensed		Upgrade	2	
Global VPN Client Enterprise	Not Licensed		Activate		
VPN SA	Licensed		Upgrade	50	
SonicOS Enhanced	Licensed				
Global Security Client	Not Licensed		Activate		
ViewPoint	Expired		Upgrade		23 Feb 2004

You can apply the following activation keys:  
 ANTI SPYWARE 1 YR BUNDLE ASMUJZF8  
 SNWL GAV 1 YR BUNDLE (IPS/GAV BUNDLE) GAMUJZF8

- Step 5** Click on the Gateway Anti-Virus link. The child Activation Key is automatically entered in the **New License Key** field. The child Activation Key is a different key than the parent key for the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.
- Step 6** Click **Submit**. If you have activated a FREE TRIAL version or are renewing a license, the renew screen is displayed that shows the expiration date of the current license and the expiration date of the updated license. Click **Renew**.

**Congratulations!** You have activated the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service.

If you activate the SonicWALL Gateway Anti-Virus, Anti-Spyware, and Intrusion Prevention Service subscription on mySonicWALL.com, the activation is automatically enabled on your SonicWALL security appliance within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to immediately update your SonicWALL security appliance.

## Setting Up SonicWALL Anti-Spyware Service Protection

After activating SonicWALL Anti-Spyware, the **Security Services > Anti-Spyware** page displays the configuration settings for managing the service on your SonicWALL security appliance.


Refer to the **SonicWALL Anti-Spyware Administrator's Guide** on the SonicWALL Web site: <http://www.sonicwall.com/us/Support.html> for complete configuration instructions.

## Applying SonicWALL Anti-Spyware Protection on Zones

If your SonicWALL security appliance is running SonicOS Enhanced, you can apply SonicWALL Anti-Spyware to Zones on the **Network > Zones** page to enforce SonicWALL Anti-Spyware not only between each network zone and the WAN, but also between internal zones. For example, enabling SonicWALL Anti-Spyware on the LAN zone enforces SonicWALL Anti-Spyware on all incoming and outgoing LAN traffic.

In the **Anti-Spyware Status** section of the **Security Services > Anti-Spyware Service** page, click the **Network > Zones** link to access the **Network > Zones** page. You apply SonicWALL Anti-Spyware to a zone listed on the **Network > Zones** page.

To enable SonicWALL on a zone, perform these steps:

- 
- Step 1** In the SonicWALL security appliance management interface, select **Network > Zones**. (Or from the **Anti-Spyware Status** section, on the **Security Services > Intrusion Prevention** page, click the **Network > Zones** link.) The **Network > Zones** page is displayed.
  - Step 2** In the **Configure** column in the **Zone Settings** table, click the edit icon  for the zone you want to apply SonicWALL Anti-Spyware. The **Edit Zone** window is displayed.
  - Step 3** Click the **Enable Anti-Spyware** checkbox. A checkmark appears. To disable SonicWALL Anti-Spyware, uncheck the box.
  - Step 4** Click **OK**.

You can also enable SonicWALL Anti-Spyware protection for new zones you create on the **Network > Zones** page. Clicking the **Add** button displays the **Add Zone** window, which includes the same settings as the **Edit Zone** window.







## CHAPTER 60

# Configuring SonicWALL Real-Time Blacklist

## SMTP Real-Time Black List Filtering

SMTP Real-time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP servers from which or through which spammers operate. There are a number of organizations that compile this information both for free <http://www.spamhaus.org>, and for profit <http://www.mail-abuse.com>. A well maintained list of RBL services and their efficacy can be found at <http://www.sdsc.edu/~jeff/spam/cbc.html>



**Note**

SMTP RBL is an aggressive spam filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The SonicOS implementation of SMTP RBL filtering provides a number of fine tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists via DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from 127.0.0.2 to 127.0.0.9 indicates some type of undesirability:

Blocked Response Codes
127.0.0.2 - Open Relay
127.0.0.3 - Dialup Spam Source
127.0.0.4 - Spam Source
127.0.0.5 - Smart Host
127.0.0.6 - Spamware Site
127.0.0.7 - Bad List Server
127.0.0.8 - Insecure Script
127.0.0.9 - Open Proxy Server

For example, an SMTP server with IP address 1.2.3.4 has been blacklisted by RBL list provider [sbl-xbl.spamhaus.org](http://sbl-xbl.spamhaus.org), then a DNS query to [4.3.2.1.sbl-xbl.spamhaus.org](http://4.3.2.1.sbl-xbl.spamhaus.org) will provide a 127.0.0.4 response, indicating that the server is a known source of spam, and the connection will be dropped.

**Note**

Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation, unbeknownst to the hosts operator. These zombie machines rarely attempt to retry failed delivery attempts, as would be the behavior of a legitimate SMTP server. As such, once the delivery attempt is thwarted by the SonicWALL RBL filter, no subsequent delivery attempts for that same piece of spam will be made.

## Security Services > RBL Filter

When **Enable Real-time Black List Blocking** is enabled on the **Security Services > RBL Filter** page, inbound connections from hosts on the WAN, or outbound connections to hosts on the WAN are checked against each enabled RBL service with a DNS request to the DNS servers configured under **RBL DNS Servers**.



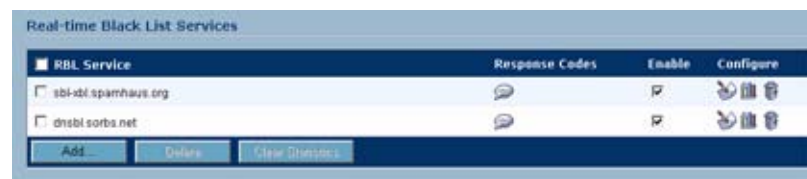
The RBL DNS Servers menu allows you to specify the DNS servers. You can choose **Inherit Settings from WAN Zone** or **Specify DNS Servers Manually**. If you select **Specify DNS Servers Manually**, enter the DNS server addresses in the **DNS Server** fields.

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server will be filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache and a DNS request must be made. In this case the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection will be dropped.

## Adding RBL Services

You can add additional RBL services the **Real-time Black List Services** section.



To add an RBL services, click the **Add** button. In the **Add RBL Domain** window, you specify the RBL domain to be queried, enable it for use, and specify its expected response codes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.



Statistics are maintained for each RBL Service in the **RBL Service** table, and can be viewed with a mouse-over of the (statistics) icon to the right on the service entry.

## User-Defined SMTP Server Lists

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow) or black-list (explicit deny) of SMTP servers. Entries in this list will bypass the RBL querying procedure. For example, to ensure that you always receive SMTP connections from a partner site's SMTP server, create an Address Object for the server you added using the **Add** button, click the edit icon in the **Configure** column of the **RBL User White List** row, and add the **Address Object**. The table will be updated, and that server will always be allowed to make SMTP exchanges.

The **System > Diagnostics** page also provides a **Real-time Black List Lookup** feature that allows for SMTP IP addresses (or RBL services, or DNS servers) to be specifically tested.

For a list of known spam sources to use in testing, refer to <http://www.spamhaus.org/sbl/latest.lasso>





## CHAPTER 61

# Configuring SonicWALL Global Security Client

---

## Security Services > Global Security Client

The SonicWALL Global Security Client combines gateway enforcement, central management, configuration flexibility and software deployment to deliver comprehensive desktop security for remote/mobile workers and corporate networks. It offers administrators the capability to manage a mobile/remote user's online access, based on corporate policies, to ensure optimal security of the network and maximize network resources. Instant messaging, high-risk Web sites and network file access can all be allowed or disallowed as security and productivity concerns dictate. Different remote/mobile users can be organized into adaptable groups with differing policies at a granular level.

SonicWALL Global Security Client delivers a low-maintenance solution to allow network administrators to secure mobile users. Residing on the remote user's system, the Global Security Client automatically communicates with an organization's SonicWALL gateway back at the office when an individual logs in to the network. Prior to allowing network access, the gateway administrator automatically updates the Global Security Client with the latest security policies and software updates. No prompting or intervention is necessary by the administrator or the remote user - it's completely seamless and transparent.

Global Security Client protection includes the SonicWALL Distributed Security Client and the SonicWALL Global VPN Client Enterprise combined with centrally managed security policies via the SonicWALL Internet Security Appliance and SonicWALL's industry-leading Distributed Enforcement Architecture (DEA).

The SonicWALL Global Security Client combines gateway enforcement, central management, configuration flexibility and software deployment to deliver comprehensive desktop security for remote/mobile workers and corporate networks. It offers administrators the capability to manage a mobile/remote user's online access, based on corporate policies, to ensure optimal security of the network and maximize network resources. Instant messaging, high-risk Web sites and network file access can all be allowed or disallowed as security and productivity concerns dictate. Different remote/mobile users can be organized into adaptable groups with differing policies at a granular level.

SonicWALL Global Security Client delivers a low-maintenance solution to allow network administrators to secure mobile users. Residing on the remote user's system, the Global Security Client automatically communicates with an organization's SonicWALL gateway back at the office when an individual logs in to the network. Prior to allowing network access, the

gateway administrator automatically updates the Global Security Client with the latest security policies and software updates. No prompting or intervention is necessary by the administrator or the remote user - it's completely seamless and transparent.

Global Security Client protection includes the SonicWALL Distributed Security Client and the SonicWALL Global VPN Client Enterprise combined with centrally managed security policies via the SonicWALL Internet Security Appliance and SonicWALL's industry-leading Distributed Enforcement Architecture (DEA).

For complete SonicWALL Global Security Client documentation, see the SonicWALL Global Security Client Administrator's Guide available at <http://www.sonicwall.com/us/Support.html>.

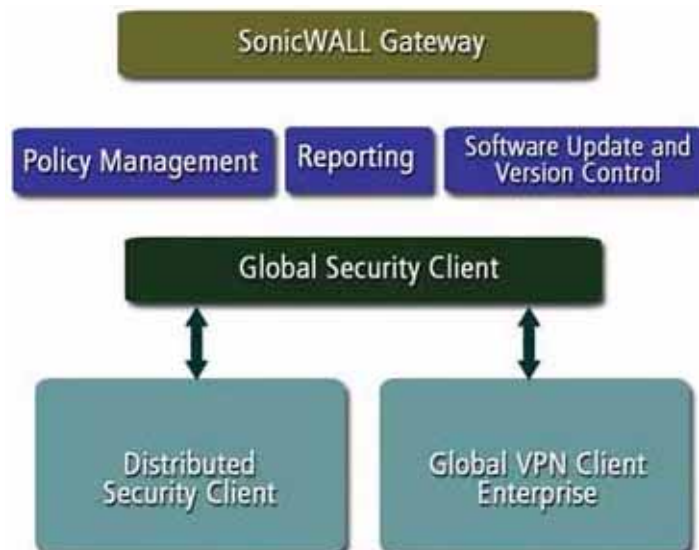
## Global Security Client Features

- **Multi-Pronged Protection** - extends the boundaries of security by protecting the corporate network and remote/mobile workers from malicious attacks that occur over the Internet.
- **Enhanced Application Security** - provides an additional layer of security by protecting organizations against legal liabilities that occur when employees accidentally or intentionally run applications from the Internet that have been designated as "untrusted" by the network administrator.
- **Policy Management** - enables network administrator's to create, distribute and manage global security policies for remote and mobile users from a central location. Once a new policy is created, it is seamlessly distributed to every system on the network with no end-user interaction required. Configuration options include specifying the minimum application version, policy levels and behavior for clients not in compliance.
- **Gateway Enforcement** - enforces security policies at the gateway to ensure the end-user's system is in compliance before being granted access to the network. Users without the Global Security Client installed on their systems must contact their administrator.
- **Scalable Architecture** - features a unique client/gateway enforcement architecture that delivers comprehensive security, scaling from the individual telecommuters and mobile users up to larger, more diverse deployments with a worldwide mobile workforce.
- **Low Total Cost of Ownership** - addresses the needs of organizations looking to deploy comprehensive desktop security to remote/mobile workers and corporate networks while delivering a lower total cost of ownership through automated policy enforcement and software distribution at the gateway.
- **Easy-to-Use Local Interface** - includes an intuitive user interface that seamlessly integrates multiple applications and presents the administrator with a status page and optional configuration functionality, offering enhanced ease of use.
- **Application Reporting** - includes application reporting to provide network administrators with data on the status of the application, as well as the ability to monitor for unusual activities and perform troubleshooting.
- **Multi-Pronged Protection** - extends the boundaries of security by protecting the corporate network and remote/mobile workers from malicious attacks that occur over the Internet.
- **Enhanced Application Security** - provides an additional layer of security by protecting organizations against legal liabilities that occur when employees accidentally or intentionally run applications from the Internet that have been designated as "untrusted" by the network administrator.

- **Policy Management** - enables network administrator's to create, distribute and manage global security policies for remote and mobile users from a central location. Once a new policy is created, it is seamlessly distributed to every system on the network with no end-user interaction required. Configuration options include specifying the minimum application version, policy levels and behavior for clients not in compliance.
- **Gateway Enforcement** - enforces security policies at the gateway to ensure the end-user's system is in compliance before being granted access to the network. Users without the Global Security Client installed on their systems must contact their administrator.
- **Scalable Architecture** - features a unique client/gateway enforcement architecture that delivers comprehensive security, scaling from the individual telecommuters and mobile users up to larger, more diverse deployments with a worldwide mobile workforce.
- **Low Total Cost of Ownership** - addresses the needs of organizations looking to deploy comprehensive desktop security to remote/mobile workers and corporate networks while delivering a lower total cost of ownership through automated policy enforcement and software distribution at the gateway.
- **Easy-to-Use Local Interface** - includes an intuitive user interface that seamlessly integrates multiple applications and presents the administrator with a status page and optional configuration functionality, offering enhanced ease of use.
- **Application Reporting** - includes application reporting to provide network administrators with data on the status of the application, as well as the ability to monitor for unusual activities and perform troubleshooting.

## How SonicWALL Global Security Client Works

The security administrator logs into the SonicWALL gateway to create security policies for all Global Security Clients using the intuitive Policy Editor interface. The Policy Editor allows the security administrator to create, edit, and deploy security policies that are automatically enforced by the SonicWALL gateway. When a remote user logs into the corporate network using the Global VPN Client Enterprise, the SonicWALL gateway seamlessly updates the user's security policy for the Distributed Security Client to ensure the client is in full compliance with corporate security policies while establishing a secure VPN connection via the Global VPN Client Enterprise.



SonicWALL's Distributed Enforcement Architecture (DEA) technology enables the policy enforcement capabilities that provide the framework for the Global Security Client's complete security solution for all remote and network desktops. SonicWALL's DEA technology enables the automatic installation of new software components, changes the configuration of different components, verifies version information, forces updates of components, informs the user which components do not meet the policy requirements, and provides user authentication for policy enforcement.

## Global Security Client Licensing

The SonicWALL Global Security Client allows you to install the Global VPN Client Enterprise and Distributed Security Client. SonicWALL Global VPN Client Enterprise is licensed on a per connection basis. That means a 5 pack of Global Security Client gives the customer 5 concurrent Global VPN Client Enterprise connections on the SonicWALL. SonicWALL Distributed Security Client licensing is licensed on a per client basis. A 5 pack of Global Security Client allows you to install Distributed Security Client on 5 computers. The Distributed Security Client license is for subscription.

If you do not have SonicWALL Global Security Client activated on your SonicWALL, you must purchase Global Security Client from a SonicWALL reseller or your mySonicWALL.com account (limited to customers in the USA and Canada only).

## Activating Global Security Client Licenses on Your SonicWALL

If you have the Activation Key for your SonicWALL Global Security Client and a mySonicWALL.com account, use the following steps to activate the Global Security Client from the SonicWALL Internet Security Appliance management interface.

- 
- Step 1** In the **System > Licenses** page of the SonicWALL Management Interface, click the [click here](#) in **To Activate, Upgrade, or Renew services** [click here](#) in the Manage Security Services Online.
  - Step 2** In the **mySonicWALL Login** page, enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System > Licenses** page appears.

Each Activation Key activates both the Global VPN Client Enterprise and Distributed Security Client licenses. You enter the Activation Key for the Distributed Security Client and the Global VPN Client Enterprise license is automatically added.
  - Step 3** Click **Upgrade** in the **Manage Service** column for **Distributed Security Client** in the **Manage Services Online** table.
  - Step 4** Type the Activation Key in the **New License Key** field for each Global Security Client (Distributed Security Client and Global VPN Client Enterprise).
  - Step 5** Click **Submit**. Your Global Security Clients are activated. The number of Global VPN Client Enterprise and Distributed Security Client licenses appear in the **Count** column of the **Manage Services Online** table on the **System > Licenses** page. The expiration date for the Distributed Security Client is displayed in the Expiration column.



## Configuring Security Policies for Global Security Clients

The **Security Services > Global Security Client** page provides the settings for configuring the security policies for Global Security Clients.

The screenshot shows the configuration page for Global Security Client. At the top, there is a navigation bar with the text "Security Services > Global Security Client" and buttons for "Apply", "Cancel", and a help icon. Below this, the page is divided into several sections:

- Global Security Client Policy:** This section displays the current policy version number being enforced, which is 0. It includes a link to "View/Edit your current GSC policy" and an "Edit Policy" button.
- Global Security Client Enforcement:** This section indicates that the Global Security Client Policy is enforced on a zone in [Network Zones](#).
- Policy excluded IP ranges:** This section features a "Range type" dropdown menu currently set to "Enforce ALL".

At the bottom of the page, there is a table with the following structure:

From Address	To Address	Configure
No Entries		

Below the table, there are two buttons: "Add" and "Delete All".



# PART 12

## Log



# CHAPTER 62

## Managing Log Events

### Log > View

The SonicWALL security appliance maintains an Event log for tracking potential security threats. This log can be viewed in the **Log > View** page, or it can be automatically sent to an e-mail address for convenience and archiving. The log is displayed in a table and can be sorted by column.

The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately e-mailed, either to an e-mail address or to an e-mail pager. Each log entry contains the date and time of the event and a brief message describing the event.

The screenshot shows the 'Log > View' interface. At the top, there are buttons for 'Refresh', 'Clear Log', 'E-Mail Log', and a help icon. Below is the 'Log View Settings' section with a table of filters and checkboxes for 'Group Filters'. The filters include Priority (All), Category (All Categories), Source (IP, Interface) (All Interfaces), and Destination (IP, Interface) (All Interfaces). The 'Filter Logic' is set to 'Priority & Category & Source & Destination'. There are buttons for 'Apply Filters', 'Reset Filters', and 'Export Log'. Below the settings is the 'Log View' section, which shows a table of log entries. The table has columns for #, Time, Priority, Category, Message, Source, Destination, Notes, and Rule. The table contains 6 entries, with some highlighted in yellow.

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
51	02/09/2006 13:36:22.832	Debug	Network Access	HTTP method detected: examining stream for host header	192.168.168.65, 1560.X0 (admin)	66.94.234.72, 80.X1	TCP HTTP	
52	02/09/2006 13:36:07.576	Alert	Intrusion Prevention	Possible port scan dropped	204.127.205.10, 80.X1	68.35.78.194, 8729.X1	TCP scanned port list: 8716, 8716, 8716, 8716, 8716	
53	02/09/2006 13:35:59.560	Notice	Network Access	TCP connection dropped	63.159.44.100, 80.X1	192.168.168.65, 1544.X0	TCP Port: 1544	
54	02/09/2006 13:34:52.176	Notice	Network Access	UDP packet dropped	65.51.65.221, 20143.X1	68.35.78.194, 1026.X1	UDP Port: 1026	
55	02/09/2006 13:34:11.560	Notice	Network Access	TCP connection dropped	64.191.192.115, 80.X1	192.168.168.65, 1531.X0	TCP Port: 1531	
56	02/09/2006 13:29:47.176	Alert	Intrusion Prevention	IPS Detection Alert: MULTIMEDIA/Multimedia Download_SIO_1212_Protech.Loz	66.250.188.141, 80.X1	192.168.168.65, 1490.X0		

## Log View Table

The log is displayed in a table and is sortable by column. The log table columns include:

- **Time** - the date and time of the event.
- **Priority** - the level of priority associated with your log event. Syslog uses eight categories to characterize messages – in descending order of severity, the categories include:
  - Emergency
  - Alert
  - Critical
  - Error
  - Warning
  - Notice
  - Informational
  - Debug

Specify a priority level on a SonicWALL security appliance on the **Log > Categories** page to log messages for that priority level, plus all messages tagged with a higher severity. For example, select 'error' as the priority level to log all messages tagged as 'error,' as well as any messages tagged with 'critical,' 'alert,' and 'emergency.' Select 'debug' to log all messages.



### Note

Refer to Log Event Messages section for more information on your specific log event.

- **Category** - the type of traffic, such as *Network Access* or *Authenticated Access*.
- **Message** - provides description of the event.
- **Source** - displays source network and IP address.
- **Destination** - displays the destination network and IP address.
- **Notes** - provides additional information about the event.
- **Rule** - notes Network Access Rule affected by event.

## Navigating and Sorting Log View Table Entries

The **Log View** table provides easy pagination for viewing large numbers of log events. You can navigate these log events by using the navigation control bar located at the top right of the **Log View** table. Navigation control bar includes four buttons. The far left button displays the first page of the table. The far right button displays the last page. The inside left and right arrow buttons moved the previous or next page respectively.

You can sort the entries in the table by clicking on the column header. The entries are sorted by ascending or descending order. The arrow to the right of the column entry indicates the sorting status. A down arrow means ascending order. An up arrow indicates a descending order.

## Refresh

To update log messages, clicking the **Refresh** button near the top right corner of the page.

## Clear Log

To delete the contents of the log, click the **Clear Log** button near the top right corner of the page.

## Export Log

To export the contents of the log to a defined destination, click the **Export Log** button below the filter table. You can export log content to two formats:

- **Plain text format**--Used in log and alert e-mail.
- **Comma-separated value (CSV) format**--Used for importing into Excel or other presentation development applications.

## E-mail Log

If you have configured the SonicWALL security appliance to e-mail log files, clicking **E-mail Log** near the top right corner of the page sends the current log files to the e-mail address specified in the **Log > Automation > E-mail** section.



### Note

The SonicWALL security appliance can alert you of important events, such as an attack to the SonicWALL security appliance. Alerts are immediately sent via e-mail, either to an e-mail address or to an e-mail pager. For sending alerts, you must enter your e-mail address and server information in the **Log > Automation** page.

## Filtering Log Records Viewed

You can filter the results to display only event logs matching certain criteria. You can filter by **Priority**, **Category**, **Destination (IP or Interface)**, and **Destination (IP or Interface)**.

**Step 1** Enter your filter criteria in the **Active Connections Monitor Settings** table.

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	<input type="text"/> X1	<input type="checkbox"/>
Destination (IP, Interface):	<input type="text"/> X0	<input type="checkbox"/>
Filter Logic:	Priority && Category && Source && Destination	
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Log"/>

**Step 2** The fields you enter values into are combined into a search string with a logical **AND**. For example, if you select an interface for **Source** and for **Destination**, the search string will look for connections matching:

Source interface AND Destination interface

**Step 3** Check the **Group** box next to any two or more criteria to combine them with a logical **OR**.

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	[ ] [X] [ ]	<input checked="" type="checkbox"/>
Destination (IP, Interface):	[ ] [ ] [X] [ ]	<input checked="" type="checkbox"/>
<b>Filter Logic:</b> (Source    Destination) && Priority && Category		
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Log"/>

For example, if you enter values for **Source IP**, **Destination IP**, and **Protocol**, and check **Group** next to **Source IP** and **Destination IP**, the search string will look for connections matching:

*(Source IP OR Destination IP) AND Protocol*

**Step 4** Click **Apply Filter** to apply the filter immediately to the **Active Connections** table. Click **Reset** to clear the filter and display the unfiltered results again.

The following example filters for log events resulting from traffic from the WAN to the LAN:

Filter	Value	Group Filters
Priority:	All	<input type="checkbox"/>
Category:	All Categories	<input type="checkbox"/>
Source (IP, Interface):	[ ] [WAN] [ ]	<input type="checkbox"/>
Destination (IP, Interface):	[ ] [ ] [LAN] [ ]	<input type="checkbox"/>
<b>Filter Logic:</b> Priority && Category && Source && Destination		
<input type="button" value="Apply Filters"/> <input type="button" value="Reset Filters"/>		<input type="button" value="Export Log"/>

#	Time	Priority	Category	Message	Source	Destination	Notes	Rule
1	02/15/2008 14:30:29.720	Alert	Intrusion Prevention	IP spoof detected	192.168.168.186, 88, WAN	255.255.255.255, 87, LAN	MAC address: 00:0b:db:5a:af:b7	
2	02/15/2008 10:00:02.304	Alert	Intrusion Prevention	IP spoof detected	192.168.168.20, 88, WAN	255.255.255.255, 87, LAN	MAC address: 00:0b:db:5a:af:b7	

## Log Event Messages

For a complete reference guide of log event messages, refer to the *SonicWALL Log Event Reference Guide* located at [http://www.sonicwall.com/us/support/230\\_3611.html](http://www.sonicwall.com/us/support/230_3611.html).



# CHAPTER 63

## Configuring Log Categories

### Log > Categories

This chapter provides configuration tasks to enable you to categorize and customize the logging functions on your SonicWALL security appliance for troubleshooting and diagnostics.



**Note**

You can extend your SonicWALL security appliance log reporting capabilities by using SonicWALL ViewPoint. ViewPoint is a web-based graphical reporting tool for detailed and comprehensive reports. For more information on the SonicWALL ViewPoint reporting tool, refer to [www.sonicwall.com](http://www.sonicwall.com).

The screenshot shows the SonicWALL web interface. The top navigation bar includes the SonicWALL logo and the text 'COMPREHENSIVE INTERNET SECURITY'. The sidebar menu on the left lists various system components: System, Network, Modem, Wireless, SonicPoint, Firewall, VoIP, VPN, Users, Security Services, and Log. The main content area is titled 'Log > Categories' and includes buttons for 'Refresh', 'Apply', and 'Cancel'. Below the title, there are configuration options for 'Log Severity/Priority' and 'Log Categories'. The 'Log Severity/Priority' section has 'Logging Level' set to 'Debug' and 'Alert Level' set to 'Alert'. The 'Log Redundancy Filter (seconds)' is set to '60' and the 'Alert Redundancy Filter (seconds)' is set to '300'. The 'Log Categories' section has 'View Style' set to 'All Categories'. Below these options is a table with the following data:

Category	Description	Log	Alerts	Syslog	Event Cou
802.11b Management	Legacy category	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	190
Attacks	Legacy category	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2
Authenticated Access	Administrator, user, and guest account activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
BOOTP	BOOTP activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
Blocked Java Etc	Legacy category	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
Blocked Web Sites	Legacy category	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0
Crypto Test	Crypto algorithm and hardware testing	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0
DDNS	Dynamic DNS activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
DMZ Client	DMZ client endpoint activity	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0

## Log Priority

This section provides information on configuring the level of priority log messages are captured and corresponding alert messages are sent through e-mail for notification.

### Logging Level

The **Logging Level** control filters events by priority. Events of equal or greater priority are passed, and events of lower priority are dropped. The **Logging Level** menu includes the following priority scale items from highest to lowest priority:

- Emergency (highest priority)
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug (lowest priority)

### Alert Level

The **Alert Level** control determines how E-mail Alerts are sent. An event of equal or greater priority causes an E-mail alert to be issued. Lower priority events do not cause an alert to be sent. Events are pre-filtered by the **Logging Level** control, so if the **Logging Level** control is set to a higher priority than that of the **Alert Level** control, only alerts at the **Logging Level** or higher are sent. Alert levels include:

- None (disables e-mail alerts)
- **Emergency** (highest priority)
- Alert
- Critical
- Error (lowest priority)

### Log Redundancy Filter

The **Log Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the SonicWALL log. Various attacks are often rapidly repeated, which can quickly fill up a log if each attack is logged. The Log Redundancy Filter has a default setting of 60 seconds.

### Alert Redundancy Filter

The **Alert Redundancy Filter** allows you to define the time in seconds that the same attack is logged on the **Log > View** page as a single entry in the SonicWALL log before an alert is issued. The Alert Redundancy Filter has a default setting of 900 seconds.

## Log Categories

SonicWALL security appliances provide automatic attack protection against well known exploits. The majority of these *legacy attacks* were identified by telltale IP or TCP/UDP characteristics, and recognition was limited to a set of fixed layer 3 and layer 4 values. As the breadth and sophistication of attacks evolved, it's become essential to dig deeper into the traffic, and to develop the sort of adaptability that could keep pace with the new threats.

All SonicWALL security appliances, even those running SonicWALL IPS, continue to recognize these legacy port and protocol types of attacks. The current behavior on all SonicWALL security appliances devices is to automatically and holistically prevent these legacy attacks, meaning that it is not possible to disable prevention of these attacks either individually or globally.

SonicWALL security appliances now include an expanded list of attack categories that can be logged.

The **View Style** menu provides the following three log category views:

- **All Categories** - Displays both **Legacy Categories** and **Expanded Categories**.
- **Legacy Categories** - Displays log categories carried over from earlier SonicWALL log event categories.
- **Expanded Categories** - Displays the expanded listing of categories that includes the older Legacy Categories log events rearranged into the new structure.

The following table describes both the Legacy and Extended log categories.

Log Type	Category	Description
802.11b Management	Legacy	Logs WLAN IEEE 802.11b connections.
Advanced Routing	Expanded	Logs messages related to RIPv2 and OSPF routing events.
Attacks	Legacy	Logs messages showing Denial of Service attacks, such as SYN Flood, Ping of Death, and IP spoofing
Authenticated Access	Expanded	Logs administrator, user, and guest account activity
Blocked Java, etc.	Legacy	Logs Java, ActiveX, and Cookies blocked by the SonicWALL security appliance.
Blocked Web Sites	Legacy	Logs Web sites or newsgroups blocked by the Content Filter List or by customized filtering.
BOOTP	Expanded	Logs BOOTP activity
Crypto Test	Expanded	Logs crypto algorithm and hardware testing
DDNS	Expanded	Logs Dynamic DNS activity
Denied LAN IP	Legacy	Logs all LAN IP addresses denied by the SonicWALL security appliance.
DHCP Client	Expanded	Logs DHCP client protocol activity
DHCP Relay	Expanded	Logs DHCP central and remote gateway activity
Dropped ICMP	Legacy	Logs blocked incoming ICMP packets.
Dropped TCP	Legacy	Logs blocked incoming TCP connections.
Dropped UDP	Legacy	Logs blocked incoming UDP packets.
Firewall Event	Extended	Logs internal firewall activity
Firewall Hardware	Extended	Logs firewall hardware error events

Log Type	Category	Description
Firewall Logging	Extended	Logs general events and errors
Firewall Rule	Extended	Logs firewall rule modifications
GMS	Extended	Logs GMS status event
High Availability	Extended	Logs High Availability activity
IPcomp	Extended	Logs IP compression activity
Intrusion Prevention	Extended	Logs intrusion prevention related activity
L2TP Client	Extended	Logs L2TP client activity
L2TP Server	Extended	Logs L2TP server activity
Multicast	Extended	Logs multicast IGMP activity
Network	Extended	Logs network ARP, fragmentation, and MTU activity
Network Access	Extended	Logs network and firewall protocol access activity
Network Debug	Legacy	Logs NetBIOS broadcasts, ARP resolution problems, and NAT resolution problems. Also, detailed messages for VPN connections are displayed to assist the network administrator with troubleshooting problems with active VPN tunnels. <b>Network Debug</b> information is intended for experienced network administrators.
Network Traffic	Expanded	Logs network traffic reporting events
PPP	Extended	Logs generic PPP activity
PPP Dial-Up	Extended	Logs PPP dial-up activity
PPPoE	Extended	Logs PPPoE activity
PPTP	Extended	Logs PPTP activity
RBL	Extended	Logs real-time black list activity
RIP	Extended	Logs RIP activity
Remote Authentication	Extended	Logs RADIUS and LDAP server activity
Security Services	Extended	Logs security services activity
SonicPoint	Extended	Logs SonicPoint activity
System Errors	Legacy	Logs problems with DNS or e-mail.
System Maintenance	Legacy	Logs general system activity, such as system activations.
User Activity	Legacy	Logs successful and unsuccessful log in attempts.
VOIP	Extended	Logs VoIP H.323/RAS, H.323/H.225, and H.323/H.245 activity
VPN	Extended	Logs VPN activity
VPN Client	Extended	Logs VPN client activity
VPN IKE	Extended	Logs VPN IKE activity
VPN IPsec	Extended	Logs VPN IPsec activity
VPN PKI	Extended	Logs VPN PKI activity
VPN Tunnel Status	Legacy	Logs status information on VPN tunnels.
WAN Failover	Extended	Logs WAN failover activity
Wireless	Extended	Logs wireless activity
Wlan IDS	Extended	Logs WLAN IDS activity

## Managing Log Categories

The **Log Categories** table displays log category information organized into the following columns:

- **Category** - Displays log category name.
- **Description** - Provides description of the log category activity type.
- **Log** - Provides checkbox for enabling/disabling the display of the log events in on the **Log > View** page.
- **Alerts** - Provides checkbox for enabling/disabling the sending of alerts for the category.
- **Syslog** - Provides checkbox for enabling/disabling the capture of the log events into the SonicWALL security appliance Syslog.
- **Event Count** - Displays the number of events for that category. Clicking the **Refresh** button updates these numbers.

You can sort the log categories in the **Log Categories** table by clicking on the column header. For example, clicking on the **Category** header sorts the log categories in descending order from the default ascending order. An up or down arrow to the left of the column name indicates whether the column is assorted in ascending or descending order.

You can enable or disable **Log**, **Alerts**, and **Syslog** on a category by category basis by clicking on the check box for the category in the table. You can enable or disable **Log**, **Alerts**, and **Syslog** for all categories by clicking the checkbox on the column header.

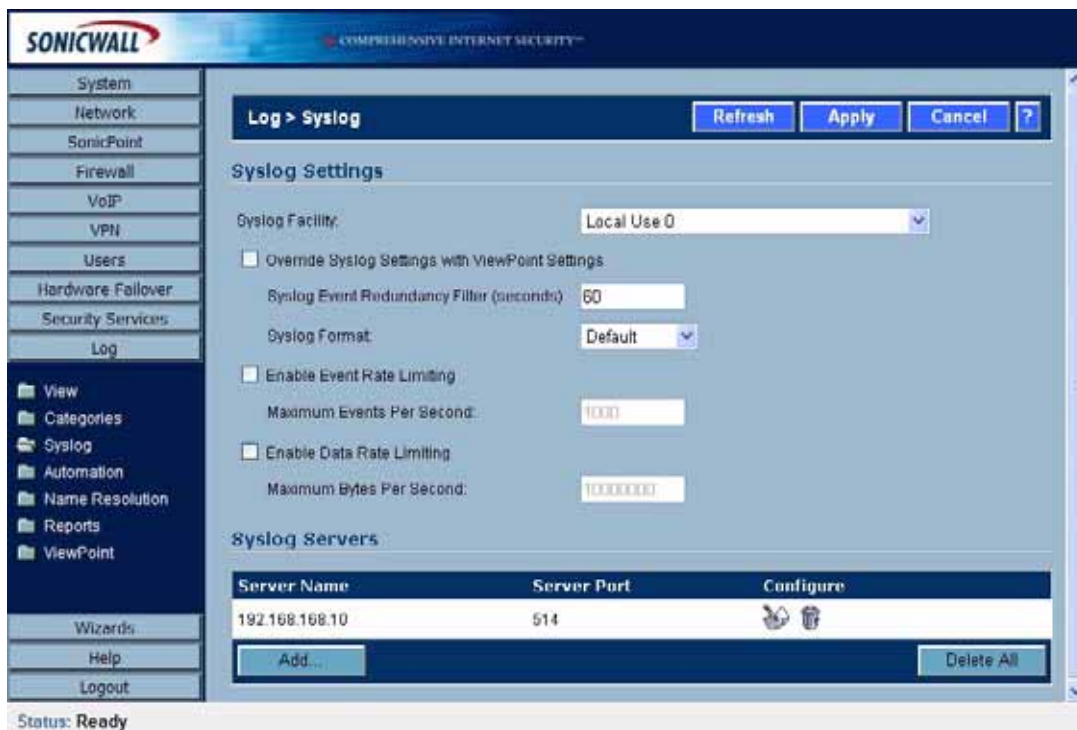


# CHAPTER 64

## Configuring Syslog Settings

### Log > Syslog

In addition to the standard event log, the SonicWALL security appliance can send a detailed log to an external Syslog server. The SonicWALL Syslog captures all log activity and includes every connection source and destination IP address, IP service, and number of bytes transferred. The SonicWALL Syslog support requires an external server running a Syslog daemon on UDP Port 514. Syslog Analyzers such as SonicWALL ViewPoint or WebTrends Firewall Suite can be used to sort, analyze, and graph the Syslog data. Messages from the SonicWALL security appliance are then sent to the server(s). Up to three Syslog server IP addresses can be added.



# Syslog Settings

## Syslog Facility

- **Syslog Facility** - Allows you to select the facilities and severities of the messages based on the syslog protocol.

**Note**

---

See RCF 3164 - The BSD Syslog Protocol for more information.

---

- **Override Syslog Settings with ViewPoint Settings** - Check this box to override Syslog settings, if you're using SonicWALL ViewPoint for your reporting solution.

**Note**

---

For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>.

---

- **Syslog Event Redundancy (seconds)** - This setting prevents repetitive messages from being written to Syslog. If duplicate events occur during the period specified in the **Syslog Event Redundancy Rate** field, they are not written to Syslog as unique events. Instead, the additional events are counted, and then at the end of the period, a message is written to the Syslog that includes the number of times the event occurred. The **Syslog Event Redundancy** default value is 60 seconds and the maximum value is 86,400 seconds (24 hours). Setting this value to 0 seconds sends all Syslog messages without filtering.
- **Syslog Format** - You can choose the format of the Syslog to be **Default** or **WebTrends**. If you select **WebTrends**, however, you must have WebTrends software installed on your system.

**Note**

---

If the SonicWALL security appliance is managed by SonicWALL GMS, the Syslog Server fields cannot be configured by the administrator of the SonicWALL security appliance.

---

- **Enable Event Rate Limiting** - This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by log events.
- **Enable Data Rate Limiting** - This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events.



# Syslog Servers

## Adding a Syslog Server

To add syslog servers to the SonicWALL security appliance

**Step 1** Click **Add**. The **Add Syslog Server** window is displayed.



**Step 2** Type the Syslog server name or IP address in the **Name or IP Address** field. Messages from the SonicWALL security appliance are then sent to the servers.

**Step 3** If your syslog is not using the default port of **514**, type the port number in the **Port Number** field.

**Step 4** Click **OK**.

**Step 5** Click **Apply** to save all **Syslog Server** settings.

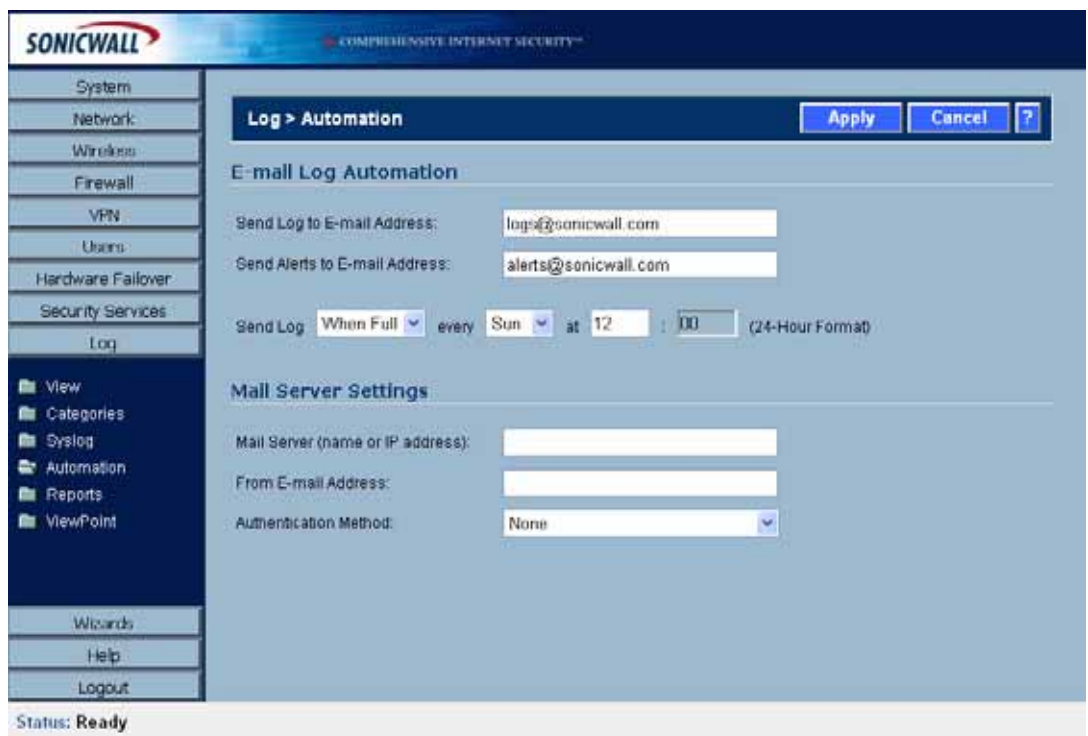


# CHAPTER 65

## Configuring Log Automation

### Log > Automation

The **Log > Automation** page includes settings for configuring the SonicWALL to send log files using e-mail and configuring mail server settings.



## E-mail Log Automation

- **Send Log to E-mail address** - Enter your e-mail address (username@mydomain.com) in this field to receive the event log via e-mail. Once sent, the log is cleared from the SonicWALL memory. If this field is left blank, the log is not e-mailed.
- **Send Alerts to E-mail address** - Enter your e-mail address (username@mydomain.com) in the **Send alerts to** field to be immediately e-mailed when attacks or system errors occur. Type a standard e-mail address or an e-mail paging service. If this field is left blank, e-mail alert messages are not sent.
- **Send Log** - Determines the frequency of sending log files. The options are **When Full**, **Weekly**, or **Daily**. If the **Weekly** or **Daily** option is selected, then select the day of the week the log is sent in the **every** menu and the time of day in 24-hour format in the **At** field.

## Mail Server Settings

The mail server settings allow you to specify the name or IP address of your mail server, the from e-mail address, and authentication method.

- **Mail Server (name or IP address)** - Enter the IP address or FQDN of the e-mail server used to send your log e-mails in this field.
- **From E-mail Address** - Enter the E-mail address you want to display in the From field of the message.
- **Authentication Method** - You can use the default None item or select **POP Before SMTP**.

**Note**

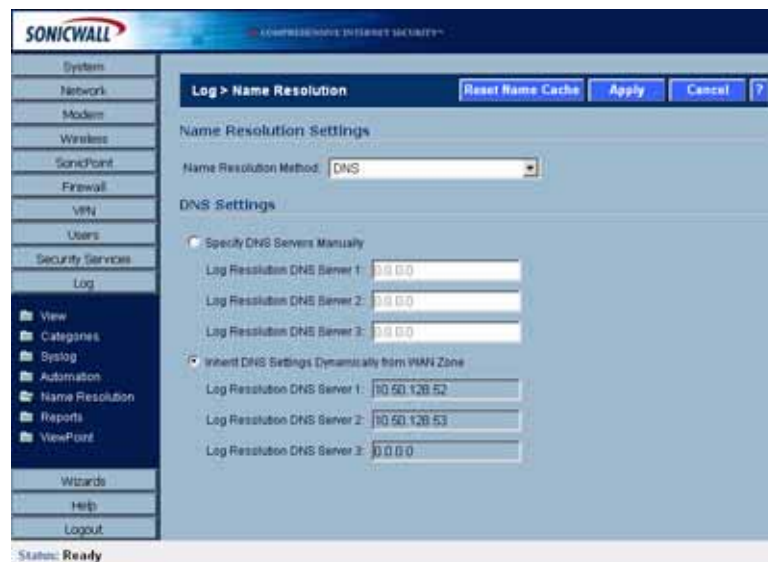
If the **Mail Server (name or IP address)** is left blank, log and alert messages are not e-mailed.

# CHAPTER 66

## Configuring Name Resolution

### Log > Name Resolution

The **Log > Name Resolution** page includes settings for configuring the name servers used to resolve IP addresses and server names in the log reports.



The security appliance uses a DNS server or NetBIOS to resolve all IP addresses in log reports into server names. It stores the names/address pairs in a cache, to assist with future lookups. You can clear the cache by clicking **Reset Name Cache** in the top of the **Log > Name Resolution** page.

### Selecting Name Resolution Settings

The security appliance can use DNS, NetBios, or both to resolve IP addresses and server names.

In the **Name Resolution Method** list, select:

- **None:** The security appliance will not attempt to resolve IP addresses and Names in the log reports.
- **DNS:** The security appliance will use the DNS server you specify to resolve addresses and names.
- **NetBios:** The security appliance will use NetBios to resolve addresses and names. If you select NetBios, no further configuration is necessary.
- **DNS then NetBios:** The security appliance will first use the DNS server you specify to resolve addresses and names. If it cannot resolve the name, it will try again with NetBios.

## Specifying the DNS Server

You can choose to specify DNS servers, or to use the same servers as the WAN zone.

- 
- Step 1** Select **Specify DNS Servers Manually** or **Inherit DNS Settings Dynamically from WAN Zone**. The second choice is selected by default.
  - Step 2** If you selected to specify a DNS server, enter the IP address for at least one DNS server on your network. You can enter up to three servers.
  - Step 3** Click **Apply** in the top right corner of the **Log > Name Resolution** page to make your changes take effect.

# CHAPTER 67

## Generating Log Reports

### Log > Reports

The SonicWALL security appliance can perform a rolling analysis of the event log to show the top 25 most frequently accessed Web sites, the top 25 users of bandwidth by IP address, and the top 25 services consuming the most bandwidth. You can generate these reports from the **Log > Reports** page.

Rank	Site	Hits
1	<a href="http://www.sonicwall.com">www.sonicwall.com</a>	103
2	<a href="http://virusscan.sag.mcafee.com">virusscan.sag.mcafee.com</a>	18
3	<a href="http://wiki.castlecorps.com">wiki.castlecorps.com</a>	15
4	<a href="http://now.eloqua.com">now.eloqua.com</a>	13
5	<a href="http://a42.mysonicwall.com">a42.mysonicwall.com</a>	13
6	<a href="http://www.nohold.net">www.nohold.net</a>	12
7	<a href="http://www.google.com">www.google.com</a>	10



**Note**

SonicWALL ViewPoint provides a comprehensive Web-based reporting solution for SonicWALL security appliances. For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>

## Data Collection

The **Reports** window includes the following functions and commands:

- **Start Data Collection**

Click **Start Data Collection** to begin log analysis. When log analysis is enabled, the button label changes to **Stop Data Collection**.

- **Reset Data**

Click **Reset Data** to clear the report statistics and begin a new sample period. The sample period is also reset when data collection is stopped or started, and when the SonicWALL security appliance is restarted.

## View Data

Select the desired report from the **Report to view** menu. The options are **Web Site Hits**, **Bandwidth Usage by IP Address**, and **Bandwidth Usage by Service**. These reports are explained below. Click **Refresh Data** to update the report. The length of time analyzed by the report is displayed in the **Current Sample Period**.

## Web Site Hits

Selecting **Web Site Hits** from the **Report to view** menu displays a table showing the URLs for the 25 most frequently accessed Web sites and the number of hits to a site during the current sample period.

The **Web Site Hits** report ensures that the majority of Web access is to appropriate Web sites. If leisure, sports, or other inappropriate sites appear in the Web Site Hits Report, you can choose to block the sites. For information on blocking inappropriate Web sites, see "[Security Services > Content Filter](#)" section on page 695.

Click on the name of a Web site to open that site in a new window.



Rank	Site	Hits
1	<a href="http://www.sonicwall.com">www.sonicwall.com</a>	827
2	<a href="http://www.malwarefilter.com">www.malwarefilter.com</a>	85
3	<a href="http://a12.mysonicwall.com">a12.mysonicwall.com</a>	55
4	<a href="http://sonicwall.mediaroom.com">sonicwall.mediaroom.com</a>	42
5	<a href="http://now.eloqua.com">now.eloqua.com</a>	34
6	<a href="http://www.sonicwall.de">www.sonicwall.de</a>	19
7	<a href="http://virusscan.san.mcafee.com">virusscan.san.mcafee.com</a>	18
8	<a href="http://gha.hitbox.com">gha.hitbox.com</a>	16
9	<a href="http://www.nvhold.net">www.nvhold.net</a>	15
10	<a href="http://wiki.castlesoft.com">wiki.castlesoft.com</a>	15
11	<a href="http://www.google.com">www.google.com</a>	10
12	<a href="http://www.kaspersploit.com">www.kaspersploit.com</a>	5
13	<a href="http://lact.hitsprocessor.com">lact.hitsprocessor.com</a>	4
14	<a href="http://a12.sonicwall.com">a12.sonicwall.com</a>	3
15	<a href="http://gha.hitbox.com">gha.hitbox.com</a>	2



## Bandwidth Usage by IP Address

Selecting **Bandwidth Usage by IP Address** from the **Report to view** menu displays a table showing the IP Address of the 25 top users of Internet bandwidth and the number of megabytes transmitted during the current sample period.



Rank	Address	Sent/Received Data
1	192.168.168.65	10 MBytes
2	192.168.168.168	321 KBytes

## Bandwidth Usage by Service

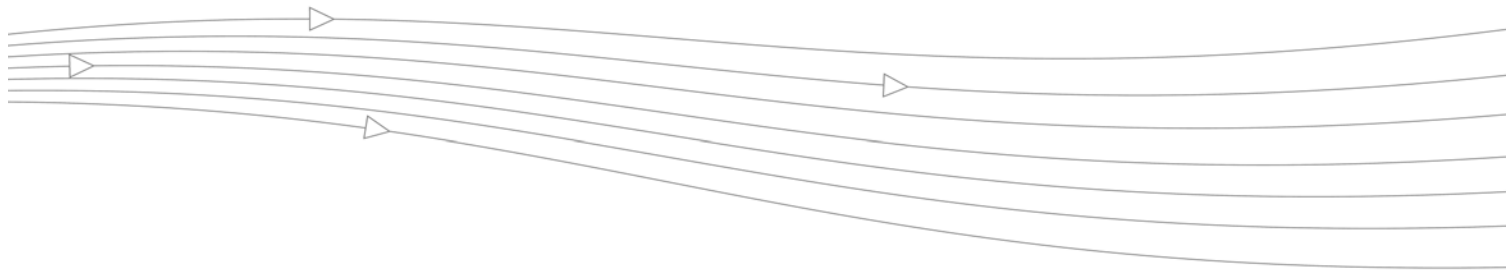
Selecting **Bandwidth Usage by Service** from the **Report to view** menu displays a table showing the name of the 25 top Internet services, such as HTTP, FTP, RealAudio, etc., and the number of megabytes received from the service during the current sample period.

The **Bandwidth Usage by Service** report shows whether the services being used are appropriate for your organization. If services such as video or push broadcasts are consuming a large portion of the available bandwidth, you can choose to block these services.



Rank	Service	Sent/Received Data
1	HTTP (6,60)	0 MBytes
2	HTTPS (6,443)	1 MBytes
3	DNS (Name Service) UDP (17,53)	8 KBytes
4	ISAKMP (17,500)	4 KBytes
5	UDP Port 0 (17,0)	0 Bytes





## CHAPTER 68

# Activating SonicWALL ViewPoint

---

## Log > ViewPoint

SonicWALL ViewPoint is a Web-based graphical reporting tool that provides unprecedented security awareness and control over your network environment through detailed and comprehensive reports of your security and network activities. ViewPoint's broad reporting capabilities allow administrators to easily monitor network access and Internet usage, enhance security, assess risks, understand more about employee Internet use and productivity, and anticipate future bandwidth needs.

ViewPoint creates dynamic, real-time and historical network summaries, providing a flexible, comprehensive view of network events and activities. Reports are based on syslog data streams received from each SonicWALL appliance through LAN, Wireless LAN, WAN or VPN connections. With ViewPoint, your organization can generate individual or aggregate reports about virtually any aspect of appliance activity, including individual user or group usage patterns, events on specific appliances or groups of appliances, types and times of attacks, resource consumption and constraints, and more.

For more information on SonicWALL ViewPoint, go to <http://www.sonicwall.com>.

For complete SonicWALL ViewPoint documentation, go to the SonicWALL documentation Web site at <http://www.sonicwall.com/us/support/3340.html>.

## Activating ViewPoint

The **Log > ViewPoint** page allows you to activate the ViewPoint license directly from the SonicWALL Management Interface using two methods.



If you received a license activation key, enter the activation key in the Enter upgrade key field, and click **Apply**.



**Warning**

**You must have a mySonicWALL.com account and your SonicWALL security appliance must be registered to activate SonicWALL ViewPoint for your SonicWALL security appliance.**

1. Click the **Upgrade** link in **Click here to Upgrade** on the **Log > ViewPoint** page. The **mySonicWALL.com Login** page is displayed.

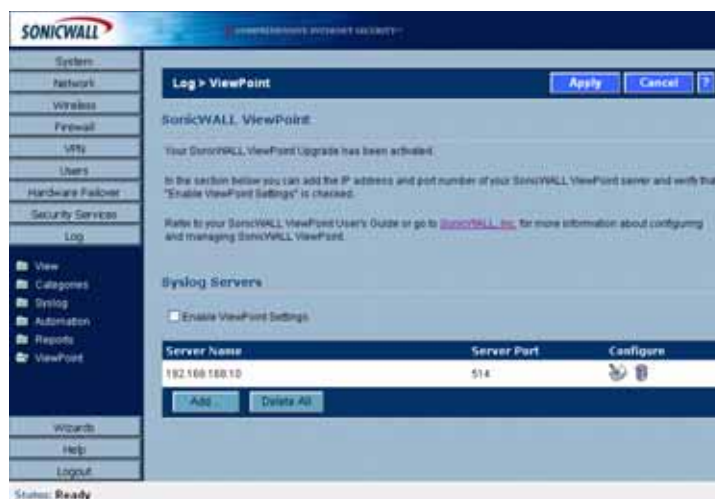


2. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**. The **System > Licenses** page is displayed. If your SonicWALL security appliance is already connected to your mySonicWALL.com account, the **System > Licenses** page appears after you click the **SonicWALL Content Filtering Subscription** link.

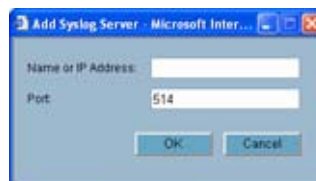
3. Click **Activate** or **Renew** in the **Manage Service** column in the **Manage Services Online** table. Type in the Activation Key in the **New License Key** field and click **Submit**.
4. If you activated SonicWALL ViewPoint at mySonicWALL.com, the SonicWALL ViewPoint activation is automatically enabled on your SonicWALL within 24-hours or you can click the **Synchronize** button on the **Security Services > Summary** page to update your SonicWALL.

## Enabling ViewPoint Settings

Once you have installed the SonicWALL ViewPoint software, you can point the SonicWALL security appliance to the server running ViewPoint.



1. Check the **Enable ViewPoint Settings** checkbox in the **Syslog Servers** section of the **Log > ViewPoint** page.
2. Click the **Add** button. The **Add Syslog Server** window is displayed.



3. Enter the IP address or FQDN of the SonicWALL ViewPoint server in the **Name or IP Address** field.
4. Enter the port number for the SonicWALL ViewPoint server traffic in the **Port** field or use the default port number.
5. Click **Apply**.



**Note**

The **Override Syslog Settings with ViewPoint Settings** control on the **Log > Syslog** page is automatically checked when you enable ViewPoint from the **Log > ViewPoint** page. The IP address or FQDN you entered in the **Add Syslog Server** window is also displayed on the **Log > Syslog** page as well as in the **Syslog Servers** table on the **Log > ViewPoint** page.

Clicking the Edit icon displays the **Add Syslog Server** window for editing the ViewPoint server information. Clicking the Delete (Trashcan) icon, deletes the ViewPoint syslog server entry.



# **PART 13**

# **Wizards**







## CHAPTER 69

# Configuring Internet Connectivity Using the Setup Wizard

---

## Wizards > Setup Wizard

The first time you log into the SonicWALL, the **Setup Wizard** is launched automatically. To launch the **Setup Wizard** at any time from the Management Interface, log into the SonicWALL. Click **Wizards** and select **Setup Wizard**.



Tip

---

You can also configure all your WAN and network settings on the **Network > Settings** page of the SonicWALL Management Interface

---

## Using the Setup Wizard

The Setup Wizard helps you configure the following settings:

- WAN networking mode and WAN network configuration (All SonicWALL security appliances)
- LAN network configuration

The **Setup Wizard** screens change depending on the choices you make. For example, if you choose Guest Internet Gateway, The **Setup Wizard** will display the screens for Modem, WAN, WLAN, and Wireless Guest Services setup. It will not display the screens for LAN and WiFiSec setup, because they do not apply in a Guest Internet Gateway deployment.





## Configuring a Static IP Address with NAT Enabled

Using NAT to set up your SonicWALL eliminates the need for public IP addresses for all computers on your LAN. It is a way to conserve IP addresses available from the pool of IPv4 addresses for the Internet. NAT also allows you to conceal the addressing scheme of your network. If you do not have enough individual IP addresses for all computers on your network, you can use NAT for your network configuration.

Essentially, NAT translates the IP addresses in one network into those for a different network. As a form of packet filtering for firewalls, it protects a network from outside intrusion from hackers by replacing the internal (LAN) IP address on packets passing through a SonicWALL with a “fake” one from a fixed pool of addresses. The actual IP addresses of computers on the LAN are hidden from outside view.

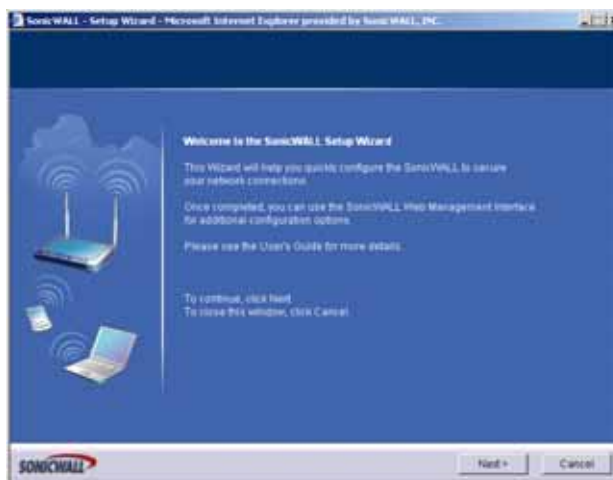
This section describes configuring the SonicWALL appliance in the NAT mode. If you are assigned a single IP address by your ISP, follow the instructions below.



**Tip**

Be sure to have your network information including your WAN IP address, subnet mask, and DNS settings ready. This information is obtained from your ISP.

## Start the Setup Wizard



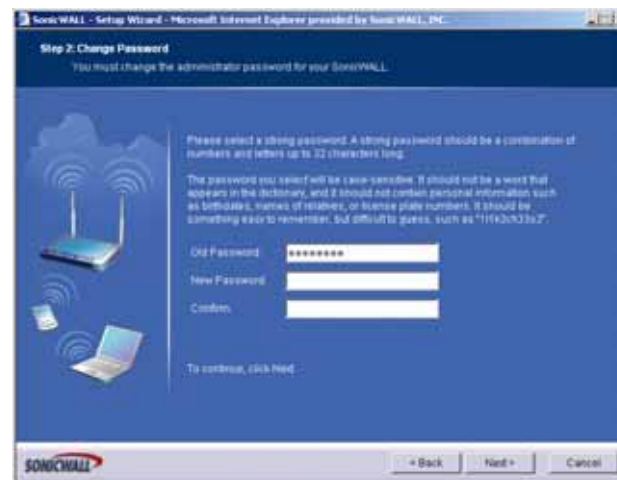
**Note**

Your Web browser must be Java-enabled and support HTTP uploads in order to fully manage SonicWALL. Internet Explorer 5.0 and above as well as Netscape Navigator 4.0 and above meet these criteria.

1. Click the **Setup Wizard** button on the **Network > Settings** page. Read the instructions on the **Welcome** window and click **Next** to continue.



## Change Password

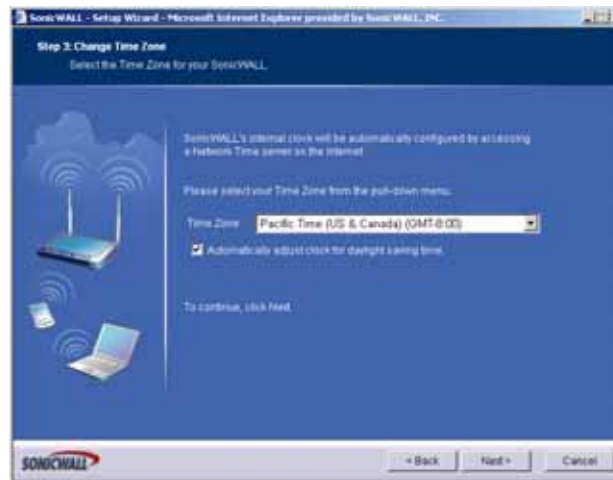


2. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.

**Tip**

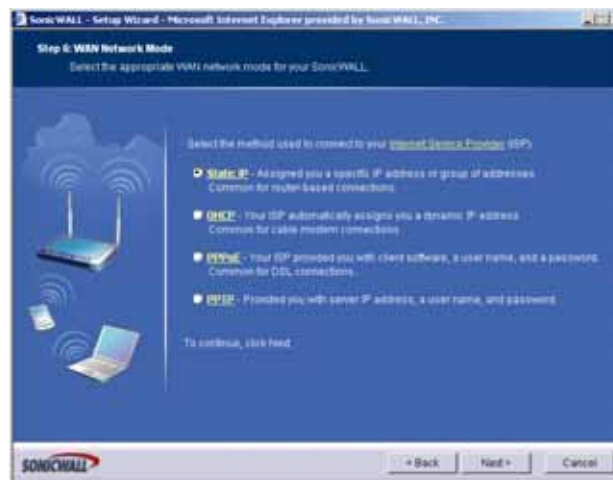
It is very important to choose a password which cannot be easily guessed by others.

## Change Time Zone



3. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

## WAN Network Mode



4. Confirm that you have the proper network information necessary to configure the SonicWALL to access the Internet. Click the hyperlinks for definitions of the networking terms.

You can choose:

- **Static IP**, if your ISP assigns you a specific IP address or group of addresses.
  - **DHCP**, if your ISP automatically assigns you a dynamic IP address.
  - **PPPoE**, if your ISP provided you with client software, a user name, and a password.
  - **PPTP**, if your ISP provided you with a server IP address, a user name, and password.
5. Choose **Static IP** and click **Next**.

## WAN Network Mode: NAT Enabled



6. Enter the public IP address provided by your ISP in the **SonicWALL WAN IP Address**, then fill in the rest of the fields: **WAN/OPT/DMZ Subnet Mask**, **WAN Gateway (Router) Address**, and **DNS Server Addresses**. Click **Next**.

## LAN Settings



7. The **LAN** page allows the configuration of the **SonicWALL LAN IP Addresses** and the **LAN Subnet Mask**. The **SonicWALL LAN IP Addresses** are the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL work for most networks. If you do not use the default settings, enter your preferred private IP address and subnet mask in the fields. Click **Next**.

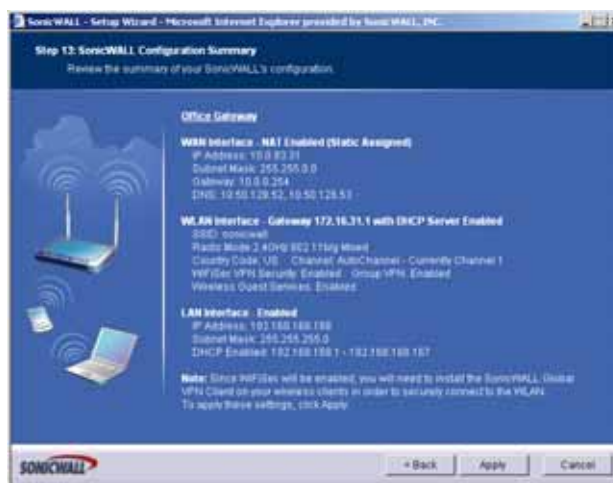
## LAN DHCP Settings



- The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically configures the IP settings of computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

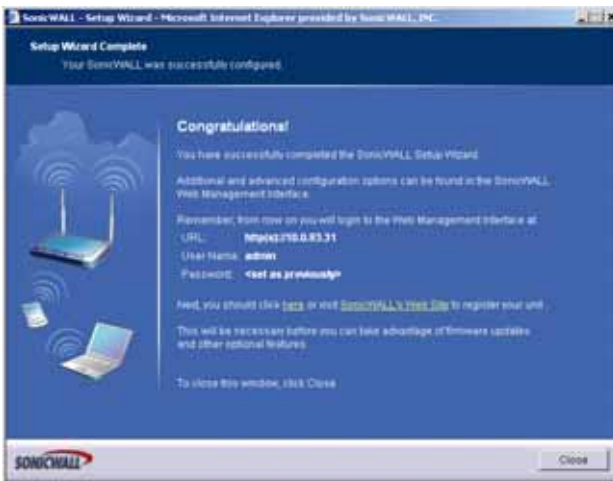
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

## SonicWALL Configuration Summary



- The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.

## Setup Wizard Complete



10. The SonicWALL stores the network settings.
11. Click **Close** to return to the SonicWALL Management Interface.

## Configuring DHCP Networking Mode

DHCP is a networking mode that allows you to obtain an IP address for a specific length of time from a DHCP server. The length of time is called a lease which is renewed by the DHCP server typically after a few days. When the lease is ready to expire, the client contacts the server to renew the lease. This is a common network configuration for customers with cable or DSL modems. You are not assigned a specific IP address by your ISP.

1. Click the **Setup Wizard** button on the **Network > Settings** page.



2. Read the instructions on the **Welcome** window and click **Next** to continue.



## Change Password



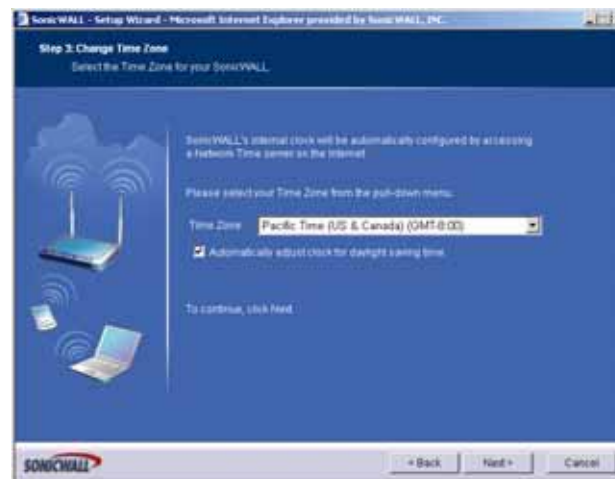
3. To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



**Tip**

It is very important to choose a password which cannot be easily guessed by others.

## Change Time Zone



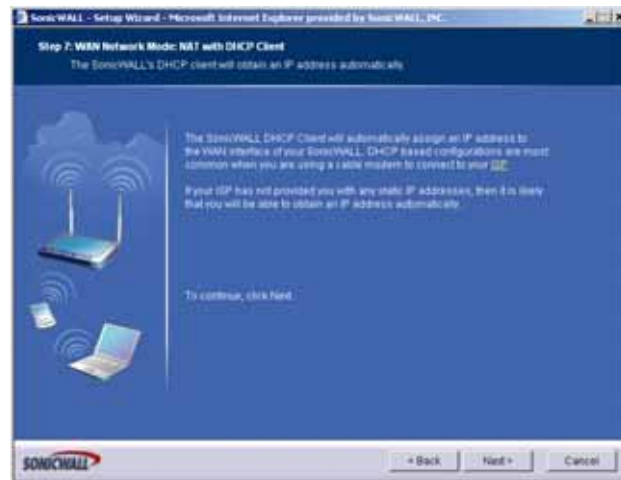
4. Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

## WAN Network Mode



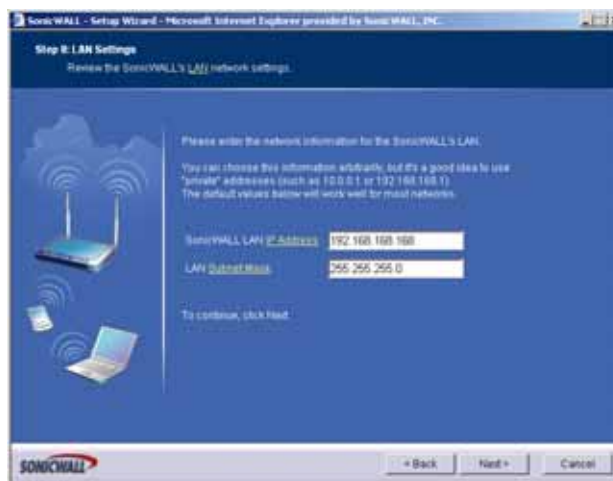
5. Select **DHCP**, the **Obtain an IP address automatically** window is displayed. Click **Next**.

## WAN Network Mode: NAT with DHCP Client



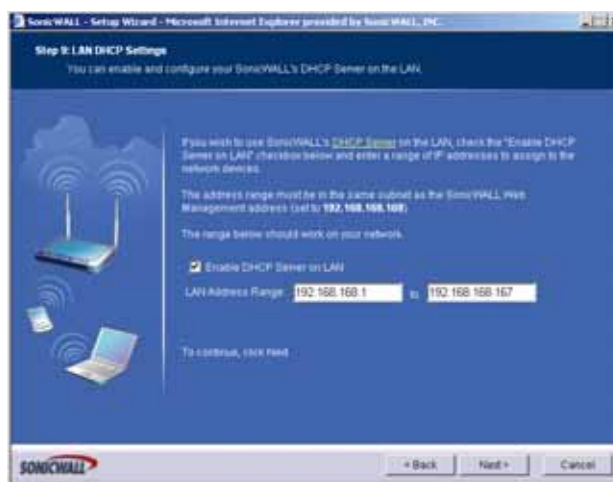
6. The **Obtain an IP address automatically** window states that the ISP dynamically assigns an IP address to the SonicWALL. To confirm this, click **Next**. DHCP-based configurations are most common with cable modem connections.

## LAN Settings



- The **Fill in information about your LAN** page allows the configuration of SonicWALL LAN IP Addresses and Subnet Masks. SonicWALL LAN IP Addresses are the private IP addresses assigned to the LAN of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the networks. The default values provided by the SonicWALL are useful for most networks. Click **Next**.

## DHCP Settings



- The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses assigned to computers on the LAN.

If **Enable DHCP Server** is not selected, the DHCP Server is disabled. Click **Next** to continue.

## SonicWALL Configuration Summary



- The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.

## Setup Wizard Complete



- The SonicWALL stores the network settings.
- Click **Close** to return to the SonicWALL Management Interface.



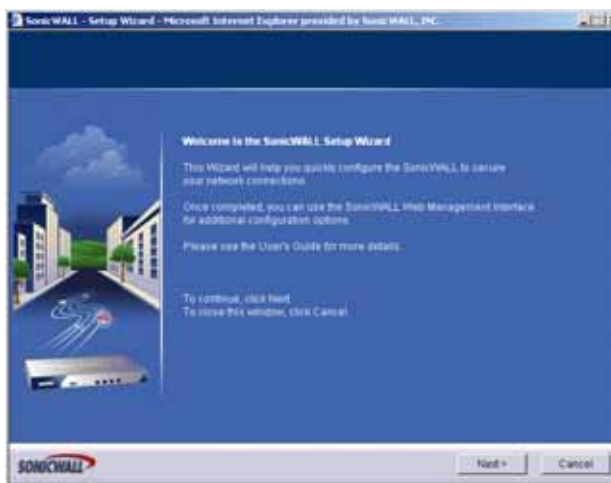
**Tip**

The new SonicWALL LAN IP address, displayed in the **URL** field of the **Congratulations** window, is used to log in and manage the SonicWALL.

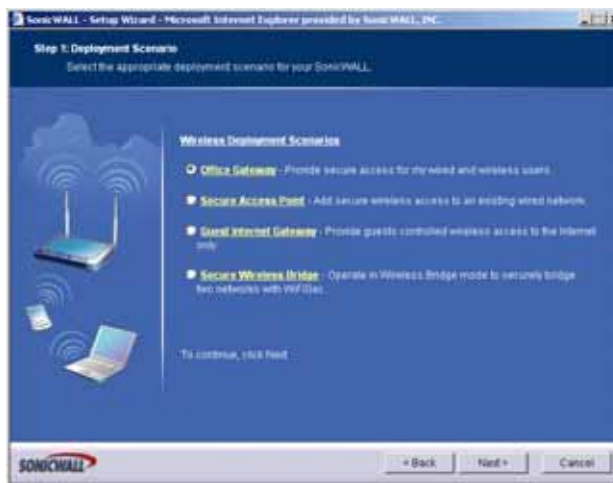
## Configuring NAT Enabled with PPPoE

**NAT with PPPoE Client** is a network protocol that uses Point to Point Protocol over Ethernet to connect with a remote site using various Remote Access Service products. This protocol is typically found when using a DSL modem with an ISP requiring a user name and password to log into the remote server. The ISP may then allow you to obtain an IP address automatically or give you a specific IP address.

1. Click the **Setup Wizard** button on the **Network > Settings** page.



2. Read the instructions on the **Welcome** window and click **Next** to continue.



## Change Password



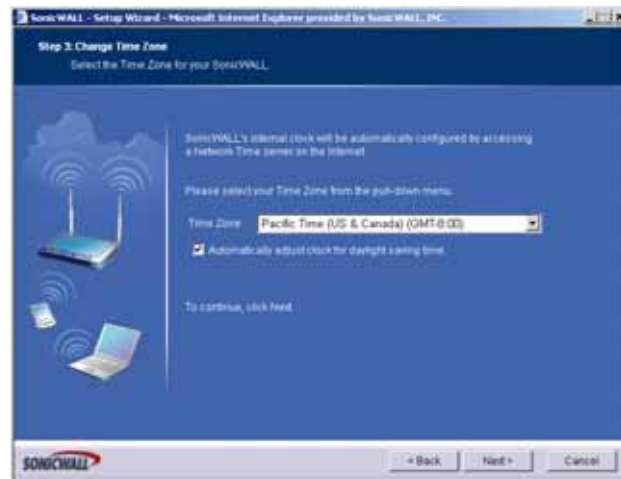
- To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



**Tip**

It is very important to choose a password which cannot be easily guessed by others.

## Change Time Zone



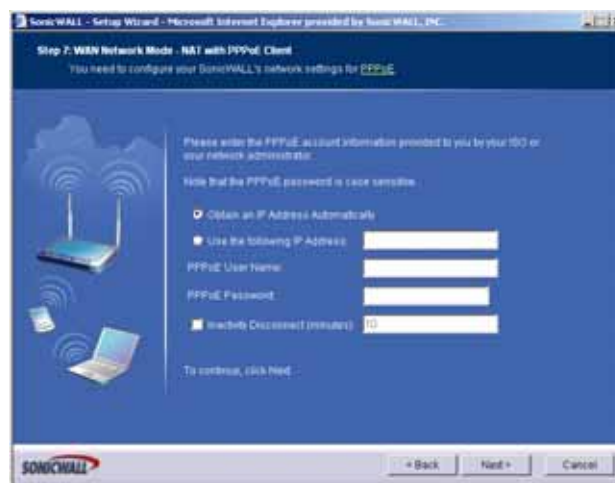
- Select the appropriate **Time Zone** from the **Time Zone** menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click **Next**.

## WAN Network Mode



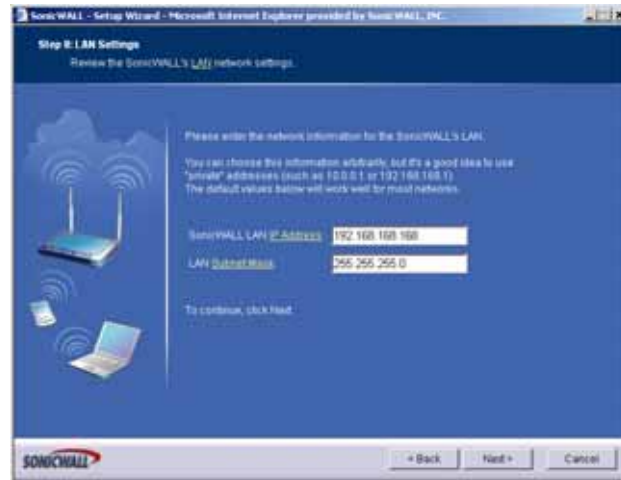
5. The SonicWALL automatically detects the presence of a PPPoE server on the WAN. If not, then select **PPPoE: Your ISP provided you with desktop software, a user name and password**. Click **Next**.

## WAN Network Mode: NAT with PPPoE Client



6. Select whether to use a dynamic or static IP address, and enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

## LAN Settings



- The **LAN Settings** page allows the configuration of SonicWALL LAN IP Addresses and LAN Subnet Mask. The SonicWALL LAN IP Address is the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

## DHCP Server



- The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.



## SonicWALL Configuration Summary



9. The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.

## Setup Wizard Complete

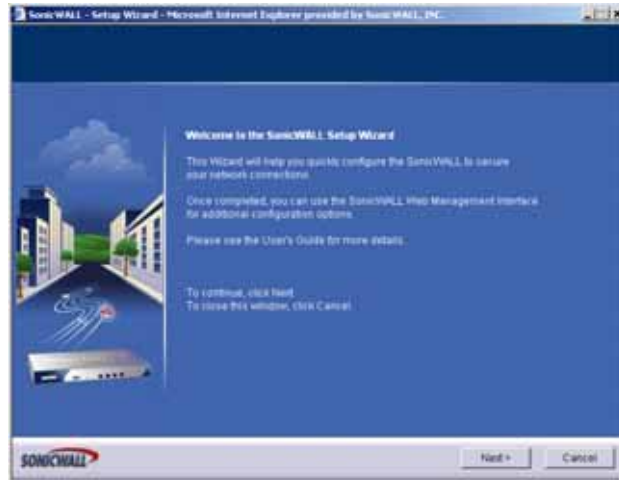


10. The SonicWALL stores the network settings.
11. Click **Close** to return to the SonicWALL Management Interface.

## Configuring PPTP Network Mode

**NAT with PPTP Client** mode uses Point to Point Tunneling Protocol (PPTP) to connect to a remote server. It supports older Microsoft implementations requiring tunneling connectivity.

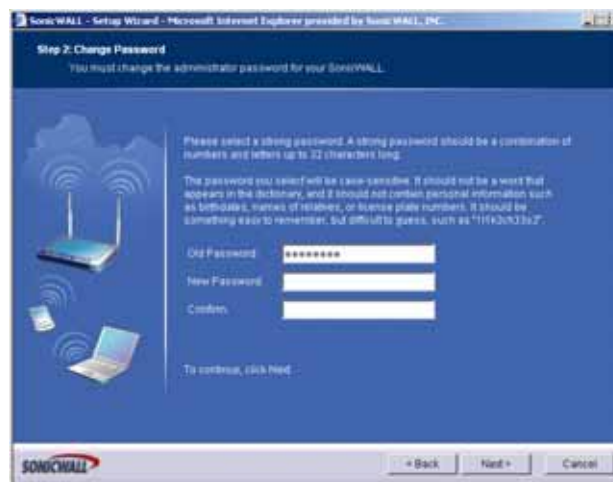
1. Click the **Setup Wizard** button on the **Network > Settings** page.



2. Read the instructions on the **Welcome** window and click **Next** to continue.



## Change Password



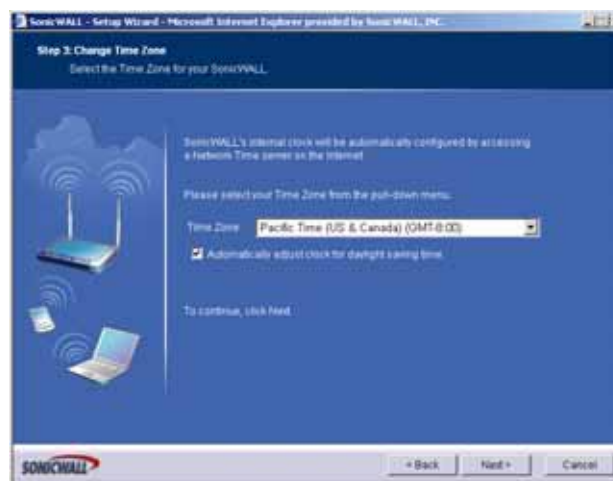
- To set the password, enter a new password in the **New Password** and **Confirm New Password** fields. Click **Next**.



**Tip**

It is very important to choose a password which cannot be easily guessed by others.

## Change Time Zone



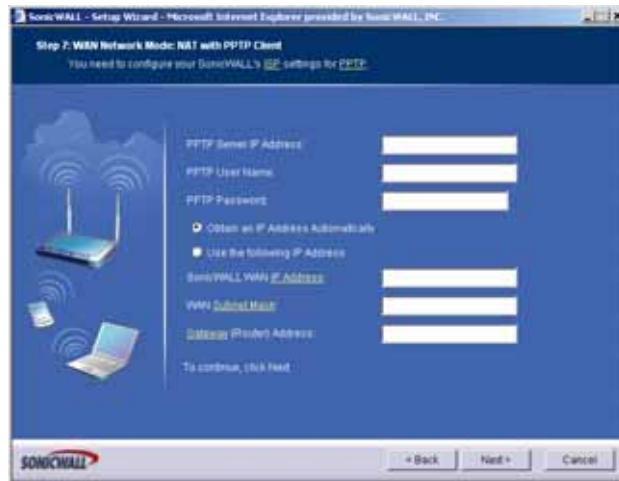
Select the appropriate Time Zone from the Time Zone menu. The SonicWALL internal clock is set automatically by a Network Time Server on the Internet. Click Next.

## WAN Network Mode



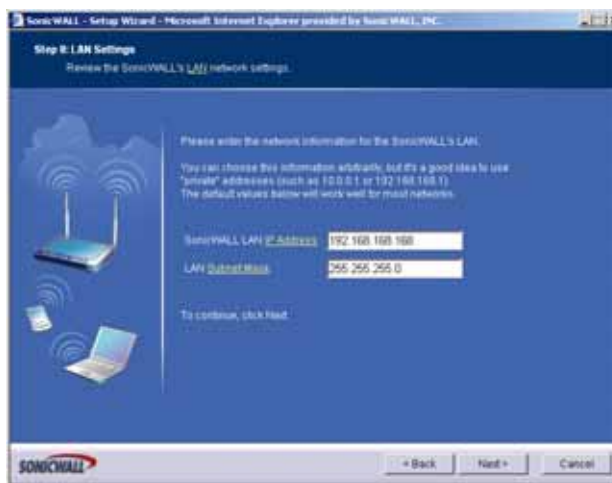
4. Select **PPTP: Provided you with a server IP address, a user name and password**. Click **Next**.

## WAN Network Mode: NAT with PPTP Client



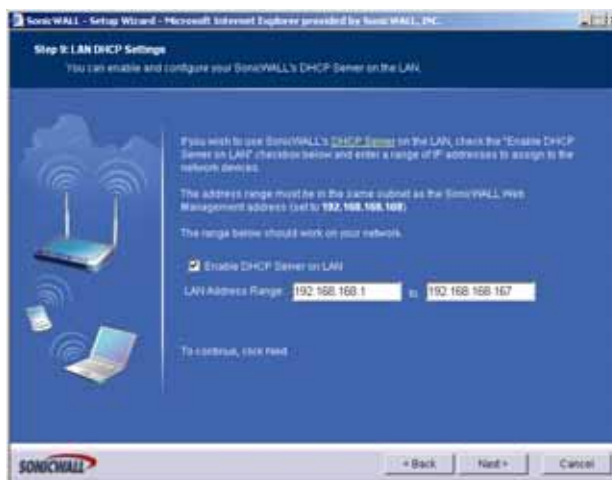
5. Enter the user name and password provided by your ISP into the **User Name** and **Password** fields. Click **Next**.

## LAN Settings



- The **LAN Settings** page allows the configuration of SonicWALL LAN IP Addresses and LAN Subnet Mask. The SonicWALL LAN IP Address is the private IP address assigned to the LAN port of the SonicWALL. The **LAN Subnet Mask** defines the range of IP addresses on the LAN. The default values provided by the SonicWALL are useful for most networks. If you do not use the default settings, enter your preferred IP addresses in the fields. Click **Next**.

## DHCP Server



- The **Optional-SonicWALL DHCP Server** window configures the SonicWALL DHCP Server. If enabled, the SonicWALL automatically assigns IP settings to computers on the LAN. To enable the DHCP server, select **Enable DHCP Server**, and specify the range of IP addresses that are assigned to computers on the LAN.

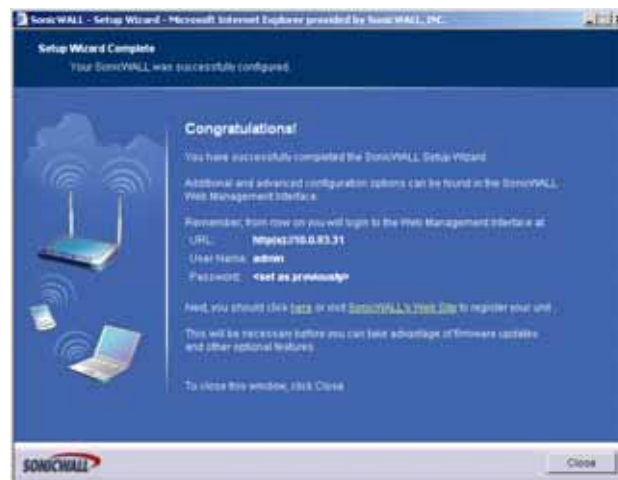
If **Disable DHCP Server** is selected, you must configure each computer on your network with a static IP address on your LAN. Click **Next**.

## SonicWALL Configuration Summary



8. The **Configuration Summary** window displays the configuration defined using the Installation Wizard. To modify any of the settings, click **Back** to return to the **Connecting to the Internet** window. If the configuration is correct, click **Next**.

## Setup Wizard Complete



9. The SonicWALL stores the network settings.
10. Click **Close** to return to the SonicWALL Management Interface.

# CHAPTER 70

## Using the Registration & License Wizard

### Wizards > Registration & License Wizard

The SonicWALL Registration and License Wizard simplifies the process of registering your SonicWALL security appliance and obtaining licenses for additional security services. To use the Registration and License Wizard, complete the following steps:

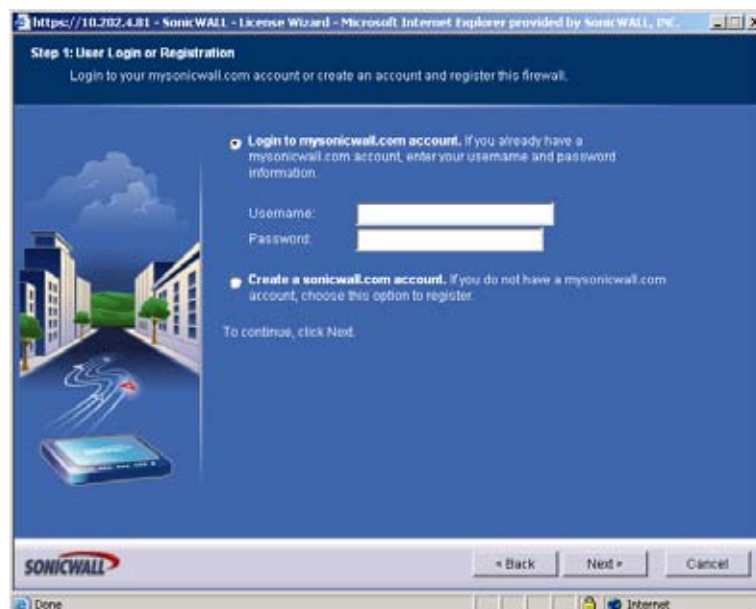
- Step 1** Launch the SonicWALL Configuration Wizard window by clicking **Wizards** in the left navigation panel.



**Step 2** Select **Registration and License Wizard** and click **Next**.

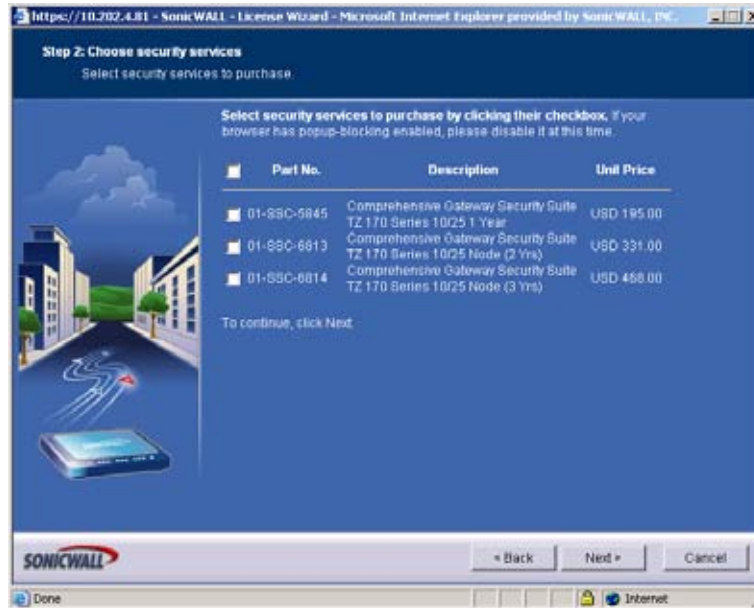


**Step 3** A screen displays confirming that you are using the Registration and License Wizard. Click **Next**.

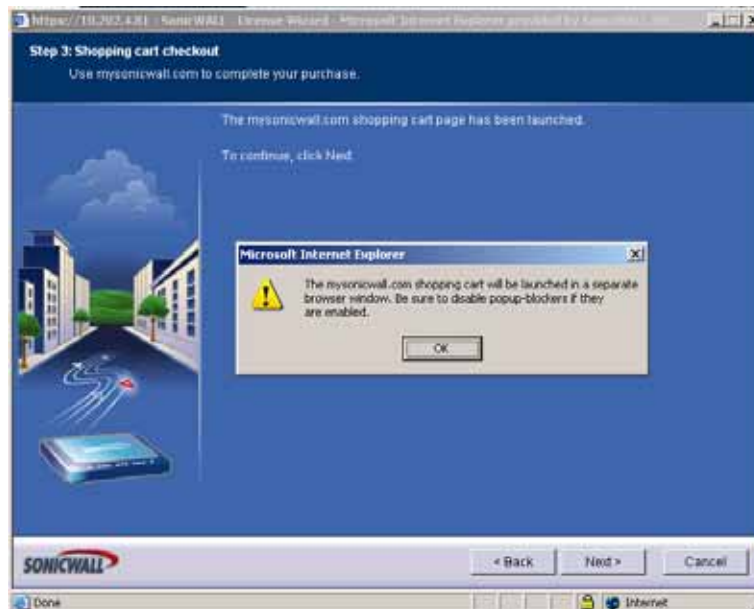


**Step 4** If you already have a mysonicwall.com account, enter your username and password. Click **Next**. If you do not have a mysonicwall.com account, select **Create a sonicwall.com account** and click **Next**. Complete the fields on the **User Registration** page to create a mysonicwall.com account and click **Next**.

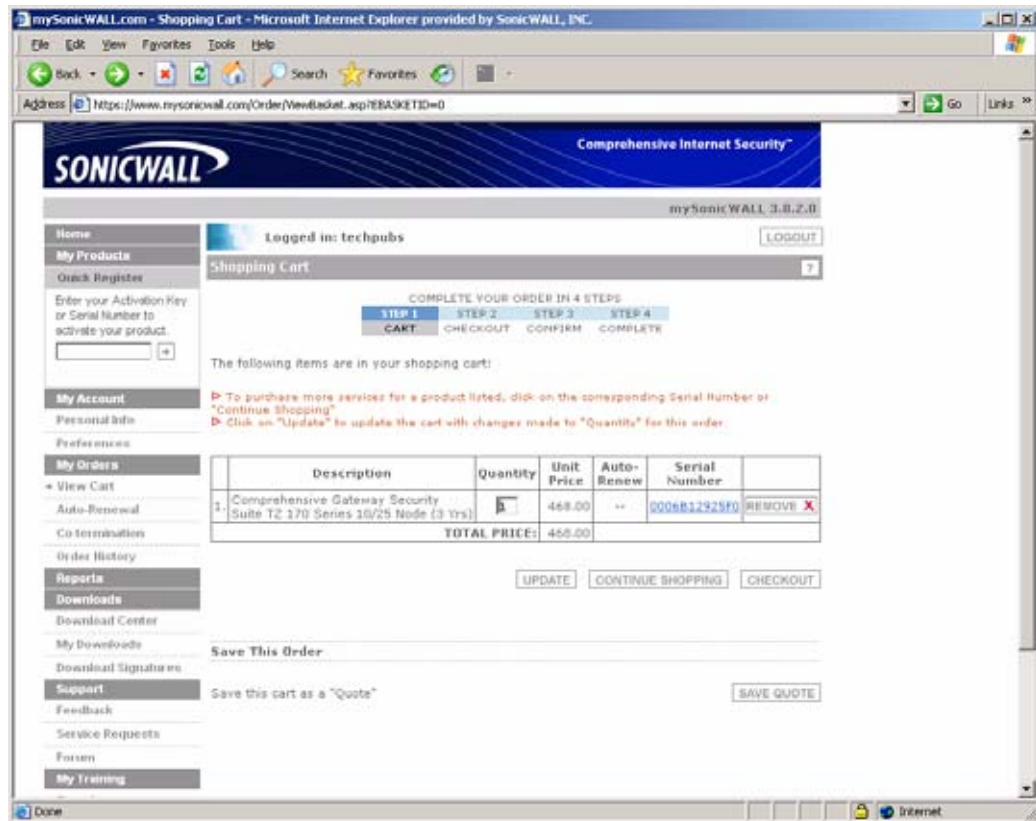




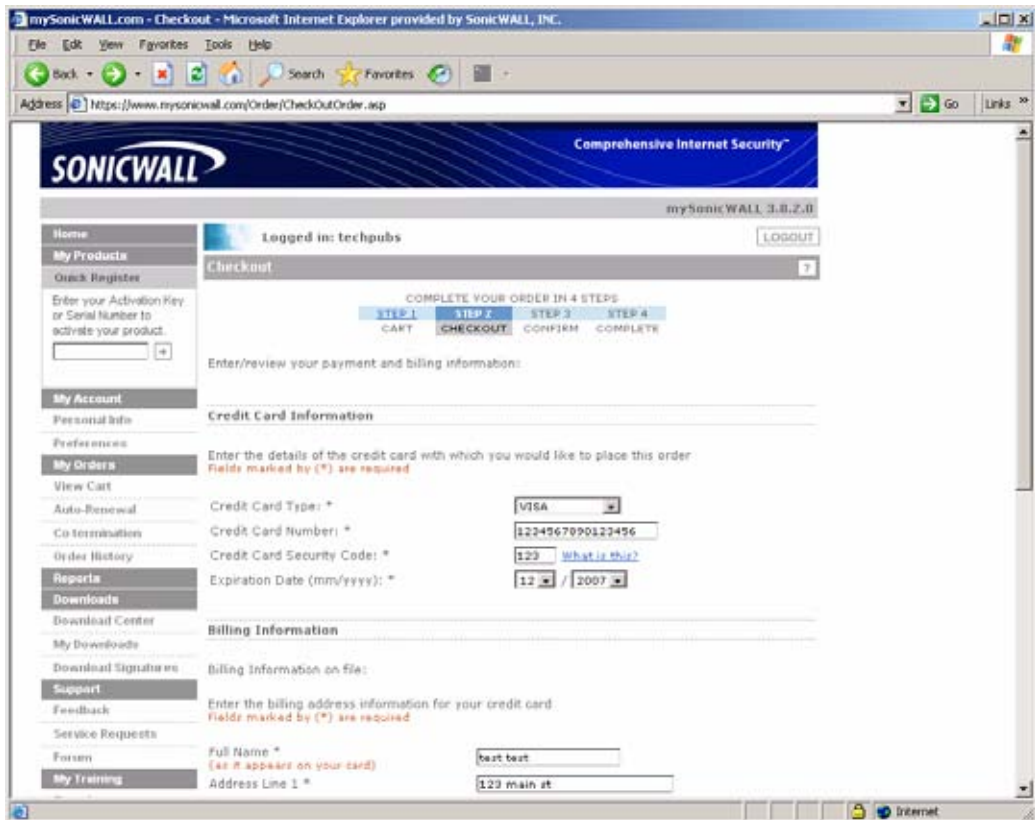
**Step 5** On the **Choose security services** page, select the security services you would like to purchase and click **Next**.



**Step 6** The **Registration and License Wizard** launches your mysonicwall.com shopping cart. Make sure that your pop-up blocker is turned off.

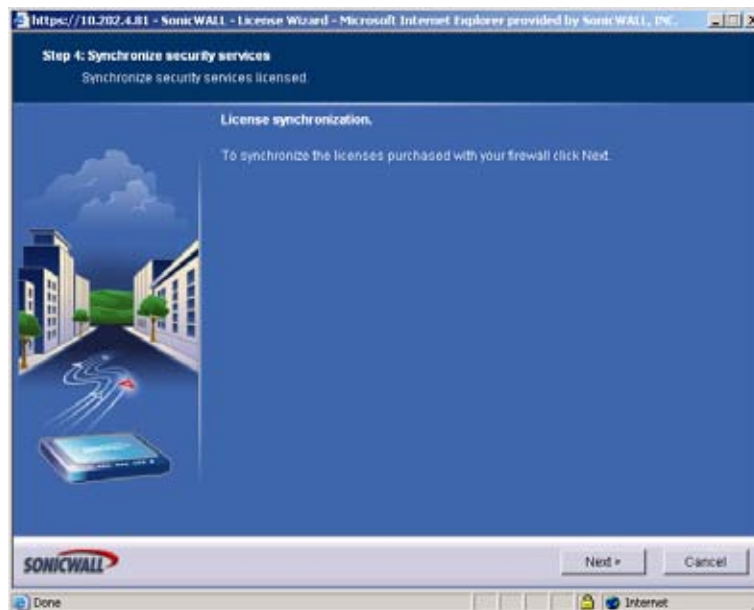


- Step 7** Verify that the services you want to purchase are listed in the shopping cart. When you are finished selecting security services, click **Checkout**.
- Step 8** The mysonicwall.com checkout page displays. Enter your credit card and billing information and click **Confirm**.

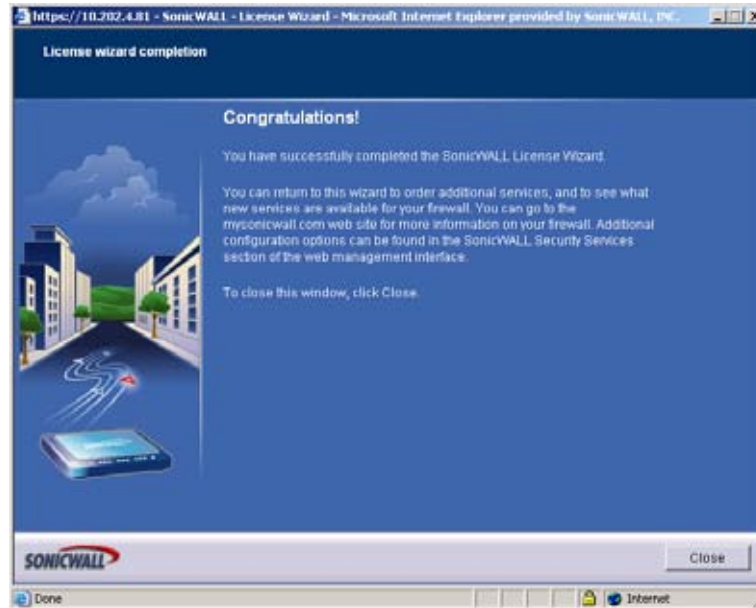


**Step 9** The Confirm page displays. Verify that your order is correct and click **Confirm**. You can now print a copy of your completed order.

**Step 10** Close the mysonicwall.com window and return to the Registration and License Wizard.



**Step 11** Click **Next** to synchronize your newly purchased licenses. The SonicWALL security appliance synchronizes with mysonicwall.com.



**Step 12** Your new security services are now available on the SonicWALL security appliance. Click **Close** to close the wizard.



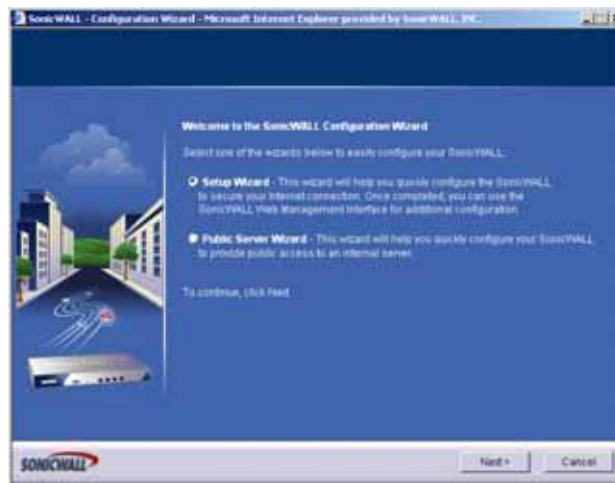
## CHAPTER 71

# Configuring a Public Server with the Wizard

---

## Wizards > Public Server Wizard

1. Start the wizard: In the navigator, click **Wizards**.



2. Select **Public Server Wizard** and click **Next**.



3. Select the type of server from the **Server Type** list. Depending on the type you select, the available services change. Check the box for the services you are enabling on this server. Click **Next**



4. Enter the name of the server.
5. Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to zone where you want to put this server. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs.

6. Click **Next**.

## 7. Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

8. Click **Next**.

9. The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:



- Server Address Objects

The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the DMZ, the wizard binds the address object to the DMZ zone. It gives the object a name of the name you specified for the server plus “\_private”. If you specify an IP in the range of another zone, it will bind the address object to that zone. If you specify an IP address out of the range of any zone you have configured, the wizard will bind the address object to the LAN zone.

Because the server in the example used the default WAN IP address for the **Server Public IP Address**, the wizard states that it will use the existing WAN address object when constructing policies between the new server and the WAN. If you specify another address, the server will create an object for that address bound to the WAN zone and assign the new address object a name of the name you specified for the server plus “\_public”.

- Server Service Group Object

The wizard creates a service group object for the services used by the new server. Because the server in the example is a web server, the service group includes HTTP and HTTPS. This way, you have a convenient group to refer to when creating or editing access policies for this server.

- Server NAT Policies

The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. Therefore, in this example, if a packet with service type of HTTPS comes in addressed to the WAN interface (10.0.93.43), the NAT policy will translate its address to 172.22.2.44.

The wizard also creates a Loopback NAT policy to translate HTTP and HTTPS traffic from inside your network addressed to the WAN IP address back to the address of the mail server.

- Server Access Rules

The wizard creates an access policy allowing all mail traffic service traffic from the WAN zone to the DMZ.



10. Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWALL.



**Tip**

The new IP address used to access the new server, internally and externally is displayed in the **URL** field of the **Congratulations** window.



11. Click **Close** to close the wizard.





## CHAPTER 72

# Configuring VPN Policies with the VPN Policy Wizard

---

### Wizards > VPN Wizard

The **VPN Policy Wizard** walks you step-by-step through the configuration of GroupVPN on the SonicWALL. After the configuration is completed, the wizard creates the necessary VPN settings for the selected VPN policy. You can use the SonicWALL Management Interface for optional advanced configuration options.

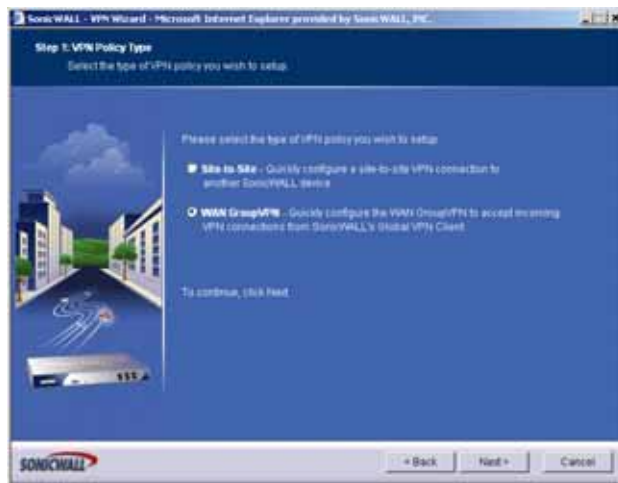
## Using the VPN Policy Wizard

**Step 1** In the top right corner of the **VPN > Settings** page, click on **VPN Policy Wizard**.

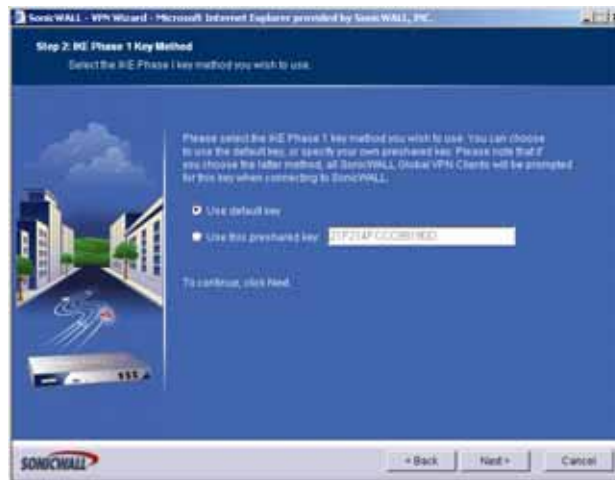


**Step 2** Click **Next**.

**Step 3** In the **VPN Policy Type** page, select **WAN GroupVPN** and click **Next**.



**Step 4** In the **IKE Phase 1 Key Method** page, you select the authentication key to use for this VPN policy:



- **Default Key:** If you choose the default key, all your Global VPN Clients and Global Security Clients will automatically use the default key generated by the SonicWALL to authenticate with the SonicWALL.
- **Use this Key:** If you choose a custom preshared key, you must distribute the key to every VPN Client because the user is prompted for this key when connecting to the SonicWALL.



**Note** If you select Use this Key, and leave the default key as the value, you must still distribute the key to your VPN clients.

**Step 5** Click **Next**.

**Step 6** In the **IKE Security Settings** page, you select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the defaults settings.



- **DH Group:** The Diffie-Hellman (DH) groups are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.

- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel.
- **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).

**Warning**

**The SonicWALL Global VPN Client version 1.x is not capable of AES encryption, so if you chose this method, only SonicWALL Global VPN Client versions 2.x and higher will be able to connect.**

**Step 7** Click **Next**.

**Step 8** In the **User Authentication** page, select if you want the VPN Users to be required to authenticate with the firewall when they connect. If you select **Enable User Authentication**, you must select the user group which contains the VPN users. For this example, leave **Enable User Authentication** unchecked.

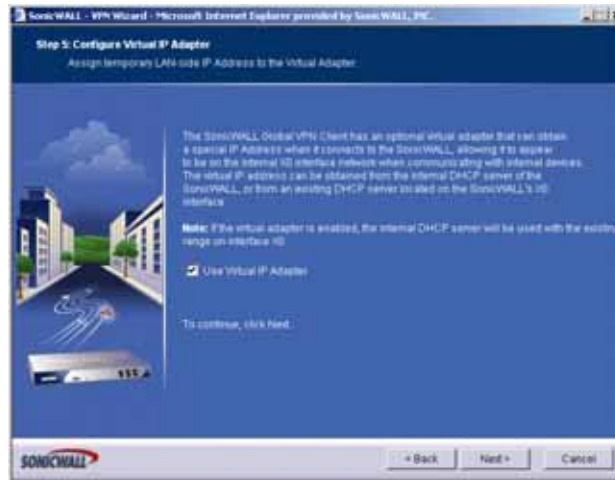


**Note**

If you enable user authentication, the users must be entered in the SonicWALL database for authentication. Users are entered into the SonicWALL database on the **Users > Local Users** page, and then added to groups in the **Users > Local Groups** page.

**Step 9** Click **Next**.

**Step 10** In the **Configure Virtual IP Adapter** page, select whether you want to use the SonicWALL's internal DHCP server to assign each VPN client IP address from the LAN zone's IP range. Therefore, when a user connects, it appears that the user is inside the LAN. Check the **Use Virtual IP Adapter** box and click **Next**.



**Step 11** The **Configuration Summary** page details the settings that will be pushed to the SonicWALL when you apply the configuration. Click **Apply** to create your GroupVPN.



## Connecting the Global VPN Clients

Remote SonicWALL Global VPN Clients install the Global VPN Client software. Once the application is installed, they use a connection wizard to setup their VPN connection. To configure the VPN connection, the client must have the following information:

- A public IP address (or domain name) of the WAN port for your SonicWALL

- The shared secret if you selected a custom preshared secret in the VPN Wizard.
- The authentication username and password.

## Configuring a Site-to-Site VPN using the VPN Wizard

You use the **VPN Policy Wizard** to create the site-to-site VPN policy.

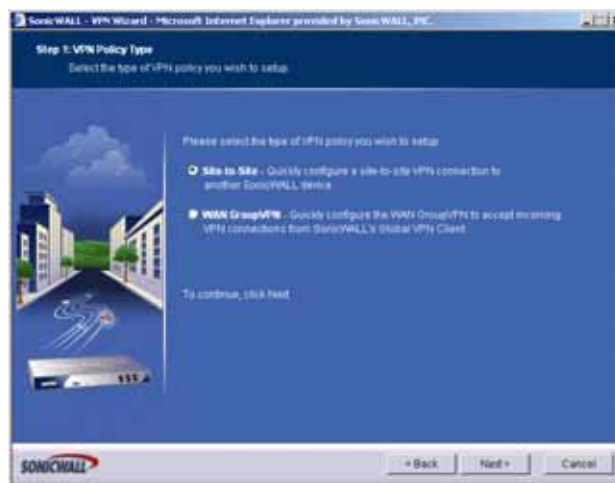


## Using the VPN Wizard to Configure Preshared Secret

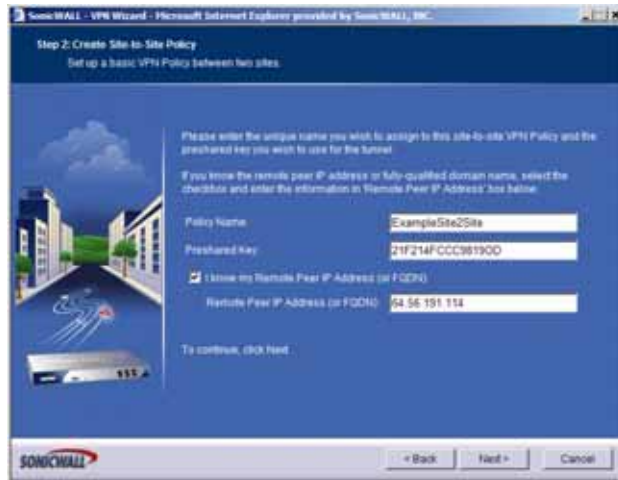
- Step 1** On the **System > Status** page, click on **Wizards**.
- Step 2** In the **Welcome to the SonicWALL Configuration Wizard** page select **VPN Wizard** and click **Next**.



- Step 3** In the **VPN Policy Type** page, select **Site-to-Site** and click **Next**.



- Step 4** In the **Create Site-to-Site Policy** page, enter the following information:



- **Policy Name:** Enter a name you can use to refer to the policy. For example, Boston Office.
- **Preshared Key:** Enter a character string to use to authenticate traffic during IKE Phase 1 negotiation. You can use the default SonicWALL generated Preshared Key.
- **I know my Remote Peer IP Address (or FQDN):** If you check this option, this SonicWALL can initiate the contact with the named remote peer.

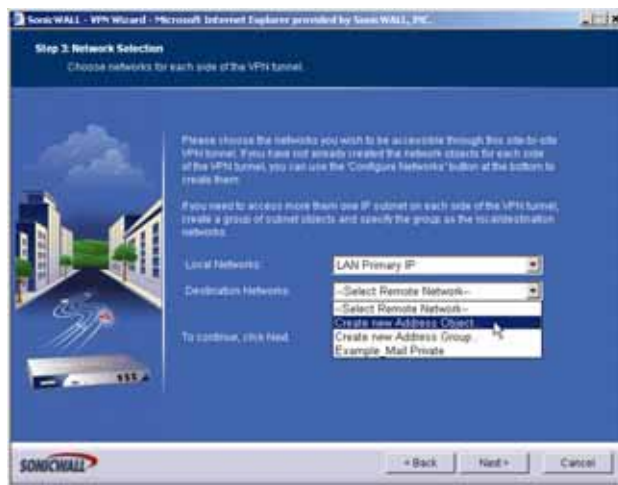
If you do not check this option, the peer must initiate contact to create a VPN tunnel. This device will use aggressive mode for IKE negotiation.

For this example, leave the option unchecked.

- **Remote Peer IP Address (or FQDN):** If you checked the option above, enter the IP address or Fully Qualified Domain Name (FQDN) of the remote peer (For example, *boston.yourcompany.com*).

**Step 5** Click **Next**.

**Step 6** In the **Network Selection** page, select the local and destination resources this VPN will be connecting:



- **Local Networks:** Select the local network resources protected by this SonicWALL that you are connecting with this VPN. You can select any address object or group on the device, including networks, subnets, individual servers, and interface IP addresses.

If the object or group you want has not been created yet, select **Create Object** or **Create Group**. Create the new object or group in the dialog box that pops up. Then select the new object or group.

For this example, select **LAN Subnets**.

- **Destination Networks:** Select the network resources on the destination end of the VPN Tunnel. If the object or group does not exist, select **Create new Address Object** or **Create new Address Group**.

For example:

- a. Select **Create new Address Group**.



- b. In the **Name** field, enter "LAN Group".
- c. In the list on the left, select **LAN Subnets** and click the -> button.
- d. Click **OK** to create the group and return to the Network Selection page.
- e. In the **Destination Networks** field, select the newly created group.

**Step 7** Click **Next**.

**Step 8** In the **IKE Security Settings** page, select the security settings for IKE Phase 2 negotiations and for the VPN tunnel. You can use the default settings.



- **DH Group:** The Diffie-Hellman (DH) group are the group of numbers used to create the key pair. Each subsequent group uses larger numbers to start with. You can choose Group 1, Group 2, or Group 5. The VPN Uses this during IKE negotiation to create the key pair.

- **Encryption:** This is the method for encrypting data through the VPN Tunnel. The methods are listed in order of security. DES is the least secure and the and takes the least amount of time to encrypt and decrypt. AES-256 is the most secure and takes the longest time to encrypt and decrypt. You can choose. DES, 3DES, AES-128, or AES-256. The VPN uses this for all data through the tunnel
- **Authentication:** This is the hashing method used to authenticate the key, once it is exchanged during IKE negotiation. You can choose MD5 or SHA-1.
- **Life Time (seconds):** This is the length of time the VPN tunnel stays open before needing to re-authenticate. The default is eight hours (28800).

**Step 9** The **Configuration Summary** page details the settings that will be pushed to the security appliance when you apply the configuration.



**Step 10** Click **Apply** to create the VPN.





# Index

---

## Symbols

401, 793, 796–797, 800–803, 805–808, 811–813, 815, 821, 827–828

## Numerics

802.11a 394  
802.11g 315, 394

## A

acceptable use policy 617  
access points  
    SonicPoints 391  
access rules  
    advanced options 430  
    bandwidth management 422  
    examples 430  
    public server wizard 824  
    viewing 423  
add 426  
address group  
    VPN policy wizard 835  
address object  
    VPN policy wizard 835  
address objects  
    about 203  
    adding 171, 209  
    creating groups 211  
    default 206  
    host 203  
    MAC address 204  
    network 203  
    public server wizard 824  
    range 203  
    types 203  
administration  
    administrator name and password 73  
    firewall name 73  
    GMS management 80  
    login security 75  
    SNMP management 78

    web management settings 77  
advance access rules 433  
advanced access rules  
    drop source routed packets 434  
    force inbound and outbound FTP data connections to  
        use default port 20 435  
    randomize IP ID 434  
    RTSP transformations 434  
    stealth mode 434  
    support for Oracle (SQLNet) 434  
    support for Windows Messenger 434  
alerts 770  
    redundancy filter 770  
ARP 272  
    ARP cache table 275  
    flushing cache 276  
    navigating and sorting entries 276  
associated stations 319  
authentication  
    VPN policy wizard 830

## B

beaconing 340

## C

CDMA, see wireless WAN  
certificates 85  
    certificate revocation list 89  
    importing 87  
    signing request 91  
CFS Exclusion List 699  
channel 319, 324  
clientless notification 730  
connection limiting 429  
consent 701  
consistent NAT 521  
content filtering service 696  
    activating 697  
    blocked message text 700  
    CFS Standard 696  
custom list 700

## D

- deep packet inspection 718
- DF bit 582
- DH group 829
  - VPN policy wizard 835
- DHCP
  - relay mode 587
  - setup wizard 797
  - VPN central gateway 588
  - VPN remote gateway 588
- DHCP over VPN
  - leases 591
- DHCP server 278
  - current leases 294
  - dynamic ranges 281
  - static entries 283
  - VoIP settings 285
- diagnostics 125
  - active connections monitor 127
  - CPU monitor 128
  - DNS name lookup 129
  - find network path 129
  - packet capture 130
  - ping 131
  - process monitor 132
  - reverse name resolution 132
  - tech support report 126
  - trace route 133
  - web server monitor 133
- Diffie-Hellman, see DH group
- Distributed Enforcement Architecture (DEA) 735
- DNS
  - configuring 201
  - inherit settings dynamically 202
  - specify DNS servers manually 201
  - with L2TP server 594
- DSL
  - setup wizard 800
- DTIM interval 342
- dynamic DNS 307
  - configuring 308
  - providers 307

## E

- easy ACL 317
- Edit Zone window 743, 751
- E-mail filter 714
- encryption
  - VPN policy wizard 830, 836
- Ethereal 106
- exclusion list
  - configuring 731

## F

- failure trigger level 582
- file transfers, restrict 728

- filter properties 700
- FIPS 104
- firmware management
  - automatic notification 100–101
  - backup firmware image 102
  - booting firmware 102
  - export settings 100
  - import settings 100
  - safemode 103
  - updating firmware 102
- fragmentation threshold 342
- fragmented packet handling 582

## G

- GAV
  - configuring 723–733
  - deep packet inspection 718
  - HTTP clientless notification 730
  - HTTP file downloads 718
  - inbound inspection 727
  - interfaces 724
  - outbound inspection 728
  - overview 715–719
  - protocol filtering 727
  - restrict file transfers 728
  - signatures 727, 732
  - SMTP messages 730
  - status information 726
  - zones 725
- Global Security Client
  - About 757
  - Activating Licenses 760
  - Features 758
  - How it Works 759
  - Licensing 760
- Global VPN Clients
  - VPN policy wizard 831
- groups
  - adding 623
  - users 620
- GSM, see wireless WAN
- guest profiles 678
- guest services 677
  - guest profile 678
  - login status window 678
- guest status 683

## H

- H.323 511
  - transforming H.323 messages 523
- hardware failover
  - wireless WAN 372–375
- HTTP clientless notification 730
- HTTP file downloads protection 718

- I**
- IDS 405
  - authorizing access points 407
  - rogue access points 406
- IEEE 802.11b 315
- IEEE 802.11g 315
- IKE
  - DH group 829
  - phase 2 835
  - VPN policy wizard 835
- IKE dead peer detection 581
- inbound inspection 727
- interclient communications 340
- interface
  - Ethernet settings 144
  - Internet traffic statistics 138
  - physical 140
- interfaces
  - bandwidth management 149
  - configuring LAN/DMZ/OPT interfaces 141, 143, 145
  - configuring WAN interface 147
  - settings 138
  - transparent mode 143
- internal network protection 717
- intrusion detection system, see IDS
- intrusion prevention service
  - architecture 736
  - deep packet inspection 735
  - terminology 736
- IP Helper 303
  - add policy 304
- ISP
  - setup wizard 800
- L**
- L2TP 593
  - configuring 594
- L2TP-over-IPSec 593
- LAN
  - setup wizard 798
- Layer 2 Tunneling Protocol, see L2TP
- local groups
  - adding 623
- local users 618
  - adding 620
  - editing 621
- log
  - automation 779
  - e-mail alert addresses 780
  - e-mailing logs 767
  - event message priority levels 768
  - exporting 767
  - generating reports 783
  - legacy attacks 771
  - log categories 773
  - mail server settings 780
  - name resolution 781
  - redundancy filter 770
  - view table 766
  - viewing events 765
- login status window 678
- logs
  - priority, configuring 770
- loopback policy 824
- M**
- MAC address 319
- MAC filter list 317, 345
- manage security services online 69
- management interface 40
  - applying changes 41
  - common icons 42
  - getting help 43
  - logging out 43
  - navigating 41
  - navigating tables 42
  - status bar 41
  - submenus 41
- mandatory filtered IP addresses 702
- MCUs 511
- multicast 457
  - create a new multicast object 458
  - IGMP state table 459
  - multicast state table entry timeout 458
  - reception of all multicast addresses 458
  - require IGMP membership reports for multicast data forwarding 458
  - snooping 458
- mySonicWALL.com
  - creating account 719
- N**
- NAT policies 245
  - comment field 249
  - creating 254
    - creating a many-to-many NAT policy 255
    - creating a many-to-one NAT policy 254
    - creating a one-to-one NAT policy for inbound traffic 257
    - creating a one-to-one NAT policy for outbound traffic 256
  - enable 249
  - inbound interface 249
  - inbound port address translation via one-to-one NAT policy 259
  - inbound port address translation via WAN (X1) IP address 260
  - navigating and sorting 246
  - original destination 248
  - original service 248
  - original source 248

- settings 248
- translated destination 248
- translated service 249
- translated source 248

- NAT policy
  - loopback policy 824
  - outbound interface 249
  - public server wizard 824
  - reflective policy 249

- NAT traversal 582
- network anti-virus 709
  - activating 710
- network settings
  - setup wizard 796

## O

- objects
  - service group 824
- open system 334
- outbound SMTP inspection 728

## P

- packet capture
  - advanced settings 119
  - basic operation 107
  - benefits 106
  - configuring 111
  - display filter 115
  - export as HTML 123
  - export as text 124
  - filter settings 112
  - FTP logging 120
  - hex dump 111
  - logging 117
  - overview 105–106
  - packet details 111
  - starting 109
  - status indicators 120
  - stopping 109
  - supported packet types 122
  - viewing packets 109

- phase 2
  - VPN policy wizard 835

- PPPoE
  - setup wizard 797

- PPTP
  - setup wizard 797

- preamble length 342

- preshared key
  - VPN policy wizard 834

- protocol filtering 727

- public server wizard 824
  - access rules 824
  - NAT policies 824
  - server address objects 824
  - server name 822

- server private IP address 822
- server type 822
- service group object 824
- starting 821

## R

- RADIUS
  - configuring user authentication 625
    - with L2TP server 594
  - registering SonicWALL security appliance 721
  - registration and license wizard 815
  - remote site protection 717
  - restart SonicWALL security appliance 134
  - restore default settings 343
  - restrict web features 698
  - rogue access points 406
  - route policies 227
  - routing 225
    - metric values 227
    - policy based routing 227
    - route advertisement 226
    - route advertisement configuration 226
    - route policies table 228
    - route policy example 229
    - static routes 225
- RTS threshold 342

## S

- SDP 399, 522
- security services
  - licenses 68
  - managing online 690
  - manual upgrade 70
  - manual upgrade for closed environments 70
  - manually update 691
  - summary 687
- server protection 718
- service group
  - public server wizard 824
- services 447
  - adding custom services 450
  - adding custom services group 454
  - default services 448
  - supported protocols 449
- settings
  - users 614
  - VPN 537
- setup wizard
  - change password 796, 801, 806, 811
  - change time zone 797, 801, 806, 811
  - configuration summary 799, 804, 809, 814
  - DHCP mode 800
  - DHCP server 808, 813
  - DHCP settings 803
  - LAN DHCP settings 799



- LAN settings 798–799, 803–804, 808, 813–814
- NAT with DHCP client 802
- NAT with PPPoE 805
- NAT with PPPoE client 807
- NAT with PPTP 810
- NAT with PPTP client 812
- static IP address with NAT enabled 795
- WAN Network mode 812
- WAN network mode 797, 802, 807
- shared key 334
- signatures 727
  - manually update 691
- signatures table 732
- SIP 511
  - media 522
  - signaling 522
  - transforming SIP messages 522
  - UDP port 523
- site-to-site VPN
  - policy name 834
  - VPN policy wizard 832
- SMTP messages, suppressing 730
- SonicPoint
  - provisioning profiles 392
  - station status 401
- SonicPoints 391
  - IDS 405
  - managing 391
- SonicWALL discovery protocol, see SDP
- SonicWALL simple provisioning protocol, see SSPP
- SonicWALL technical support 28
- SonicWALL ViewPoint 787
  - activating 787
  - enabling 789
- SSID 319
- SSID controls 340
- SSPP 399
- static IP
  - setup wizard 797
- status
  - security services 63
  - users 613
  - wireless 318
- syslog
  - adding server 777
  - event redundancy rate 776
  - server settings 776
- syslog server 775
- system
  - alerts 63
  - information 62
  - network interfaces 66
  - status 61

## T

This 421

- time
  - NTP settings 94
  - setting 93
- transmit power 342
- trusted domains 699

## U

- user authentication
  - VPN policy wizard 830
- users
  - acceptable use policy 617
  - active sessions 613, 669
  - adding 620
  - adding local groups 623
  - authentication methods 615
  - configuring RADIUS authentication 625
  - creating local groups 621
  - editing 621
  - global settings 616
  - groups 620
  - guest accounts 679
  - guest profile 678
  - guest services 677
  - guest status 683
  - local users 618
  - login status window 678
  - settings 614
  - SonicWALL authentication 620
  - status 613

## V

- virtual IP adapter
  - VPN policy wizard 831
- VPN 537, 581
  - active L2TP sessions 595
  - active tunnels 551
  - advanced settings 581
  - DF bit 582
  - DHCP leases 591
  - DHCP over VPN 587
    - central gateway 588
    - remote gateway 588
  - DHCP relay mode 587
  - export client policy 560
  - global security client 542
  - global VPN client 542
  - GroupVPN 552
  - L2TP Server 593
  - L2TP-over-IPSec 593
  - NAT traversal 582
  - planning sheet 542
  - settings 537
  - site-to-site 561
  - VPN policy window 562
  - VPN policy wizard 827
- VPN policy wizard

- authentication 830, 836
- configuration summary 836
- connecting Global VPN Clients 831
- destination networks 835
- DH group 829, 835
- encryption 830, 836
- IKE phase 1 key method 828
- IKE security settings 829, 835
- life time 836
- local networks 834
- peer IP address 834
- policy name 834
- preshared key 834
- site-to-site VPN 832
- user authentication 830
- virtual IP adapter 831
- VPN policy type 828

## W

### WAN

- GroupVPN 828

### WAN failover 181

- caveats 181
- outbound load balancing methods 184
- probe monitoring 186
- setting up 182
- statistics 189

### web proxy 305

- bypass proxy servers 306
- configuring 305

### WEP 394

- WiFiSec 315, 319

- WiFiSec enforcement 317

- WiFiSec Protected Access 337

- EAP 336, 338
- PSK 335, 337

### wireless

- IDS 405
- SonicPoints 391
- WAN, see wireless WAN

### wireless encryption

- authentication type 334
- extensible authentication protocol 335
- extensible authentication protocol 336, 338
- pre-shared key 335, 337
- WEP key 335
- WPA encryption 335

- wireless encryption protocol, see WEP

- wireless firmware 319

- wireless guest services 319

- wireless node count 317

- wireless status 318

- wireless WAN 152–157, 371–388

- CDMA 372
- configuring 377–385
- connection model 153, 372

- data limiting 384

- failover 153, 372–375

- glossary 386

- GSM 372

- maximum allowed connections 157

- maximum connection time 383

- monitoring 385

- overview 371–376

- PC cards 376

- prerequisites 376

- service providers 376

- status 377

- wireless zones 391

- Wireshark 106

### wizards

- setup wizards 793

### WLAN 319

- IP address 319

- settings 319

- statistics 320

- subnet mask 319

- WWAN, see wireless WAN

## Z

### zone

- SonicPoints 391

- wireless 391

### zones 191

- adding 196

- allow interface trust 194, 197

- enabling security services 194

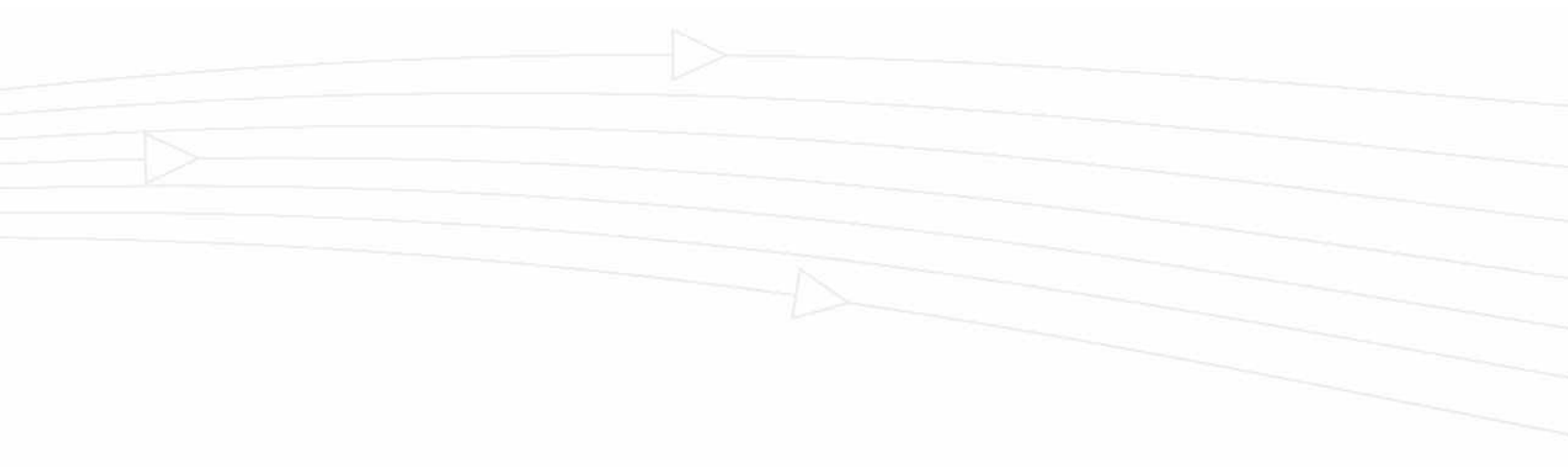
- GAV 725

- how zones work 192

- predefined 193

- security types 193

- zone settings table 195



SonicWALL, Inc.

1143 Borregas Avenue  
Sunnyvale CA 94089-1306

T +1 408.745.9600  
F +1 408.745.9300

[www.sonicwall.com](http://www.sonicwall.com)



**PN: 232-001213-00**  
**Rev A 06/08**

©2008 SonicWALL, Inc. is a registered trademark of SonicWALL, Inc. Other product names mentioned herein may be trademarks and registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.

